



6.2.4 | June 2013 | 3725-77601-001H

Polycom[®] CMA[®] System Operations Guide



Trademark Information

POLYCOM® and the names and marks associated with Polycom's products are trademarks and/or service marks of Polycom, Inc., and are registered and/or common law marks in the United States and various other countries.

All other trademarks are the property of their respective owners.



Java is a registered trademark of Oracle and/or its affiliates.

Patent Information

The accompanying product may be protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

End User License Agreement

Use of this software constitutes acceptance of the terms and conditions of the Polycom CMA system end-user license agreement (EULA).

The EULA for your version is available on the Polycom Support page for the Polycom CMA system.

© 2011-2013 Polycom, Inc. All rights reserved.

Polycom, Inc.
6001 America Center Drive
San Jose CA 95002
USA

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc. Under the law, reproducing includes translating into another language or format.

As between the parties, Polycom, Inc., retains title to and ownership of all proprietary rights with respect to the software contained within its products. The software is protected by United States copyright laws and international treaty provision. Therefore, you must treat the software like any other copyrighted material (e.g., a book or sound recording).

Every effort has been made to ensure that the information in this manual is accurate. Polycom, Inc., is not responsible for printing or clerical errors. Information in this document is subject to change without notice.

Contents

1	Polycom® CMA® System Overview	1
	Polycom CMA System Features and Capabilities	1
	Polycom CMA System Models	2
	Minimum System Requirements	2
	Working in the Polycom CMA System	3
	Log Into the Polycom CMA System	3
	Field Input Requirements	4
	Filter and Search a List	4
	Change a Password	5
	Log Out of the Polycom CMA System	6
	Restart or Shut Down a Polycom CMA System	6
	Emergency Shutdown of a Polycom CMA System	7
2	Polycom CMA System Configuration	9
	Add DNS SRV Record for Polycom CMA System Services	9
	Configure the Connection to the External Database	10
	Configure the Connection to an External Enterprise Directory	10
	Configure Redundancy	11
	Set Up Video Call Routing	11
	Set Up Automatic Provisioning	12
	Set Up Automatic Softupdate	12
	Set Up Conference Templates	12
	Set Up Directory Services	13
	Set Up a Certificate for the Polycom CMA System	13
	Distribute Polycom Applications	14
	Distribute Polycom CMA Desktop for Windows Systems	14
	Distribute Polycom CMA Desktop for MAC OS Systems	15
3	Operating in Maximum Security Environments	17
	Maximum Security Mode Overview	17
	Conference Scheduling in Maximum Security Mode	18

Endpoint Management in Maximum Security Mode	19
Network Device Management in Maximum Security Mode	20
Polycom RMX Systems in Secure Mode	21
User Management in Maximum Security Mode	21
Scheduler	21
Operator	21
Administrator	21
Group Management in Maximum Security Mode	24
Reporting in Maximum Security Mode	24
Administrator	24
Operator	25
Auditor	25
Device Administration in Maximum Security Mode	26
About Machine Accounts	26
System Administration in Maximum Security Mode	27
Admin Menu	28
Conference Templates	28
Provisioning Profiles	29
Software Updates	29
Server Settings	29
Management and Security	30
Dial Plan and Sites	33
Backup System Settings	33
Network Intrusion Detection in Maximum Security Mode	34
Troubleshooting in Maximum Security Mode	35
Troubleshooting Utilities	35
Report Administration	37

4 Polycom® CMA® System Conference Scheduling Overview . 39

Conference Menu Overview	40
Conference Menu and Views	40
Conference Views—Future and Ongoing	42
Conference States	43
Context-Sensitive Conference Actions	44
General Scheduling Information	45
Scheduling Participants and Endpoints	45
Bridge Selection and Cascading	45
Bridge Scheduling and Reassignment	46

5 Conference Scheduling Operations 49

Add/Schedule a Conference	49
Add/Schedule a New Conference	49

	Copy an Existing Conference	55
	Edit a Conference	56
	Edit a Participant's Settings	57
	View Scheduling Information for a Conference	59
6	Advanced Scheduling Operations	61
	Edit Conference Settings	61
	Select a Bridge for a Conference	67
	Create a Cascaded Conference Across Multiple Bridges	67
7	Conference and Participant Management Operations	69
	Manage an Active Conference	69
	Add Additional Participants to an Active Conference	72
	Add a Room to an Active Conference	73
	View the Video of a Participant in an Active Conference	74
	Join an Active Conference	74
	Add a Participant from a Favorites List to an Active Conference	75
	Add/Save a Participant to a Favorites List	75
	Manage a Participant's Endpoint During a Conference	76
	View a Participant's Details During a Conference	77
	Terminate an Active Conference	79
	Delete a Conference	79
8	Conference and Participant Details	81
	Conference Image	81
	Conference Details	81
	Conference Features	83
	Bridge (MCU) Features	84
	Participants List	85
	Participant Details	86
	Participant Settings	87
9	Endpoint Management Overview	89
	Endpoint Menu, Views, and Lists	89
	Monitor View	90
	Endpoint List in the Monitor View	90
	Actions in the Monitor View	92
	Peripherals View	93
	Peripherals List in the Peripherals View	93
	Actions in the Peripheral View	94

Bundled Provisioning View	95
Endpoint List in the Bundled Provisioning View	95
Actions in the Bundled Provisioning View	96
Automatic Provisioning View	96
Endpoint List in the Automatic Provisioning View	96
Actions in the Automatic Provisioning View	97
Scheduled Provisioning View	97
Endpoint List in the Scheduled Provisioning View	97
Actions in the Scheduled Provisioning View	98
Automatic Software Update View	99
Endpoint List in the Automatic Software Update View	99
Actions in the Automatic Software Update View	100
Scheduled Software Update View	101
Endpoint List in the Scheduled Software Update View	101
Scheduled Software Update View Actions	102
Endpoint Types	103
Endpoint Configuration/Provisioning	105
Provisioning Best Practices	106
Bundled Provisioning	106
How Bundled Provisioning Works	107
Automatic Provisioning	107
How Automatic Provisioning Works	108
Automatic Provisioning Profiles	109
Profile Order and Priority	113
Scheduled Provisioning	113
How Scheduled Provisioning Works	113
Scheduled Provisioning Profiles	114
Endpoint Gatekeeper Registration Policies	132
Endpoint Software Updates	133
Automatic Software Updates	133
How Automatic Software Update Works	133
Automatic Software Update Profiles	133
Automatic Software Update Versions	134
Peripheral Software Updates	135
Scheduled Software Updates	135
Endpoint Passwords	136
Considerations for Third-Party Endpoints	136
Enable TANDBERG Endpoints Global Address Book Access	137
Considerations for LifeSize Endpoints	137
Enabling Management of LifeSize Endpoints	137
Monitoring	138
Scheduled Provisioning of Selected TANDBERG Endpoints	138
Scheduled Provisioning of LifeSize Endpoints	157

Provisioning of LifeSize Passwords	164
Reporting	164
10 Endpoint and Peripheral Management Operations	165
Endpoint Management Operations	165
View Device Details	166
Add an Endpoint or Find an Endpoint on the Network	170
Edit an Endpoint	174
Delete an Endpoint	175
View an Endpoint's Video Feed	176
Clear an Endpoint Help Request	176
Send a Message to an Endpoint	177
Reboot an Endpoint	177
Associate a User with an Endpoint	177
Search for Endpoints in a Range of IP Addresses	178
View Peripherals	178
Peripheral View Operations	179
Delete Peripheral	179
Display Applications	179
11 Endpoint Provisioning Operations	181
Bundled Provisioning Operations	181
View the Provisioning Bundle List	181
Download a Provisioning Bundle	182
Delete a Provisioning Bundle	182
Automatic Provisioning Operations	183
View the Automatic Provisioning List and Details	183
Add an Automatic Provisioning Profile	183
Edit an Automatic Provisioning Profile	184
Edit the Profile Order for an Automatic Provisioning Profile	185
Clone an Automatic Provisioning Profile	185
Delete an Automatic Provisioning Profile	185
Scheduled Provisioning Operations	186
View the Scheduled Provisioning List and Details	186
Add a Scheduled Provisioning Profile	186
Edit a Scheduled Provisioning Profile	187
Clone a Scheduled Provisioning Profile	187
Delete a Scheduled Provisioning Profile	188
Schedule an Endpoint for Provisioning	188
Check the Status of a Scheduled Provisioning	189

Clear the Status of Scheduled Provisioning	189
Cancel a Scheduled Provisioning	189

12 Endpoint Software Update Operations 191

Automatic Software Update Operations	191
View Automatic Software Update Information	191
View Automatic Software Update Packages	192
Set Maintenance Window for Automatic Software Updates	193
Implement Automatic Software Updates for Endpoints	193
List the Serial Numbers for the Endpoints to be Updated	194
Download the Required Software Package	195
Request Update Activation Keys	195
Upload the Software Package and Create a Software Update Package	196
Set an Automatic Software Update Policy	197
Trial a Software Update Package	198
Create a Local Trial Group	198
Upload the Software Package and Create a Trial Software Update Package	199
Promote the Trial Software Update Package to Production	199
Delete the Trial Software Update Package	200
View and Implement Software Updates for Peripherals	200
View Software Updates for Peripherals	201
Upload Peripheral Software Updates to the CMA Web Server .	202
Configure Peripheral Updates for Production	202
Configure Peripheral Updates for Trial	204
Scheduled Software Update Operations	205
View Scheduled Software Update Information	206
View List of Software Update Packages	206
Implement Scheduled Software Updates for Endpoints	206
List the Serial Numbers for the Endpoints to be Updated	206
Download the Required Software Package	207
Request Update Activation Keys	208
Upload the Software Package and Create a Software Update Profile 209	
Schedule the Software Update for Endpoints	209
Cancel Software Updates	210

13 Device Details 213

Device Summary Information	213
Device Status Information	215
Call Information	217
Device Alerts Information	218

Provisioning Details	218
Software Update Details	219
14 Network Device Management Overview	221
Network Device Types	221
Network Device Menu, Views, and Lists	221
Monitor View	222
Network Device List in the Monitor View	222
Actions in the Monitor View	224
VBP View	224
MCU View	225
DMA View	225
15 MCU Bridge Management Operations	227
View Device Details	227
Add an MCU Manually	232
Edit an MCU Bridge	233
Enable Cascading Conferences on Polycom MCUs	234
Delete an MCU Bridge	235
View Bridge Hardware	235
View Bridge Services	236
View Bridge Conferences	236
View Bridge Ports	236
View Bridge Meeting Rooms	237
View Bridge Entry Queues	237
View Bridge Gateway Conferences	237
16 Management Operations for Other Network Devices	239
Polycom VBP Management Operations	239
Add a Polycom VBP Device	240
Copy the CMA System Certificate to a Polycom VBP Device	240
Edit a Polycom VBP Device	241
Delete a Polycom VBP Device	241
Identify Endpoints Using the Polycom VBP Device	241
Polycom DMA Management Operations	242
Add a Polycom DMA System	242
Edit a Polycom DMA System	242
Delete a Polycom DMA System	243
View Registered DMA Nodes	243

17	MCU Bridge Device Details	245
	MCU H.320 Services	245
	MCU H.323 Services	246
	MCU Gateway Services	247
	MCU Resources—Polycom MGC Platform	247
	MCU Resources—Polycom RMX Platform	248
18	Users and Groups Overview	249
	Overview of Groups, Users, and User Roles	249
	Users	249
	Local Users	249
	Enterprise Users	250
	Groups	250
	Local Groups	251
	Enterprise Groups	251
	Roles and Permissions	252
	Default CMA System Roles and Permissions	253
	Scheduler Roles, Responsibilities, and Menus	255
	Operator Role, Responsibilities, and Menus	255
	Device Administrator Role, Responsibilities, and Menus	256
	Auditor Role, Responsibilities, and Menus	257
	Administrator Role, Responsibilities, and Menus	258
	Customized Roles and Responsibilities	258
	Device Associations and Presence	259
19	User Management Operations	261
	Manage Users	261
	Search for a User	261
	View User Information	262
	Add a Local User	263
	Edit a User	265
	View Permissions for a User	266
	Delete a User	266
	Unlock a User Account	267
	Manage Groups	268
	Add a Local Group	268
	Import Enterprise Groups	269
	Edit a Group	270
	Delete a Group	270
	Manage User Roles	270

Assign Users Roles and Endpoints	272
View the List of User Roles	272
Add a User Role	273
Edit Permissions for a User Role	273
Delete a User Role	274
View the Groups and Users Associated with a User Role	274
Manage System Guest Book	275
User Menu and Guest Book	275
Context-Sensitive Guest Book Actions	276
Add a Guest to the System Guest Book	276
Edit a Guest in the System Guest Book	278
Delete a Guest from the System Guest Book	279
Manage Favorites	279
Add a Favorites List	279
Edit a Favorites List	280
Delete a Favorites List	280
20 System Reports	281
Site Statistics Report	281
Site Link Statistics Report	283
H.323 Call Detail Records Report	284
Call Detail Record Report Administration	285
Modify the CDR Retention Period	285
Schedule Weekly Archives of the CDR Report	285
Endpoint Usage Report	286
Conference Type Report	292
Gatekeeper Message Log	294
View and Export the Gatekeeper Message Log	294
Define Log Settings	295
Clear Events from the Log	296
Pause and Restart Logging	296
View and Export System Log Files	300
Change the System Log Level	300
Download Windows Event Log Files	301
View and Download Audit Log Files	301
Backup and Delete Audit Log Files	302
CMA System Report	303
21 System Administration Overview	307
Polycom CMA System Dashboard	307

	Dashboard Buttons	308
	Dashboard Panes	308
	System Administration Menu	317
22	Conference Setup Overview	321
	Conference Templates	321
	Conference Settings	334
23	Conference Setup Operations	337
	View the Conference Templates List	337
	Add a Conference Template	338
	Edit a Conference Template	338
	Delete a Conference Template	339
	Set Conference Settings	339
	Disable Conference Auto-Launch	339
	Disable Conference Time Warning	339
	Overbooking Dial-in Participants	340
	Add Customized Text to E-mail Notifications	340
	Edit Customized Text in E-mail Notifications	341
	Delete Customized Text in E-mail Notifications	341
24	Room Overview and Operations	343
	Local and Enterprise Meeting Rooms	343
	View the Rooms List	344
	Add a Local Room	344
	Add an Enterprise Room	345
	Edit a Room	346
	Delete a Room	346
25	Area Overview and Operations	347
	Areas Overview	347
	How Areas Work	347
	Area Best Practices	348
	View Areas	349
	Create Area Administrator Role	350
	Enable, Configure, and Customize Areas	350
	Add Areas	351
	Assign Devices to Areas	351
	Associate Users with Areas	352

Change Area Association for Users	353
Delete an Area	353
26 Directory Operations	355
Directory Management Overview	355
Directory Management Supported Configurations	356
Multiple Forests	356
Multiple Domains	356
Viable options:	356
Groups	356
Users	357
How Global Catalog Searches Work	358
Accounts Required for the CMA System	359
CMA System Service Account	359
CMA System Computer Account	359
Understanding Base DN	359
Understanding Exclusion Filters	361
Polycom CMA System and Windows Authentication	362
Directory Management Operations	363
Integrate with Enterprise Directory Server Option	363
Create the Polycom CMA System Service Account	364
Create the Polycom CMA System Computer Account	365
Enable Integration with the Enterprise Directory Server	366
Allow Delegated Authentication to Enterprise Directory Server ...	367
Remove or Include Dynamically-Managed Endpoints in the Global Address Book	368
Remove or Include Guest Book Entries in the Directory	369
Support LifeSize Endpoints in Directories	369
Modify Directory Listings	369
Configure LDAP Settings	370
27 Directory Setup Operations	371
View the Global Address Book	371
Set or Change the GAB Password	372
28 Multiple Address Books	373
Multiple Address Books Overview	373
How Multiple Address Books Work	374
View the Address Book List and Details	375
Add an Address Book	375
Edit an Address Book	377

Assign Address Books to Groups	379
Viewing the Address Book a User is Assigned To	380
Delete an Address Book	380
Change Address Book Priority	381
Set the Default Address Book	381
Copy an Address Book	382
 29 Polycom CMA System Setup Overview	383
Server Settings	383
Polycom CMA System Licensing	384
Polycom CMA System Site Topology and Dial Plan Set Up	386
Sites List	387
Add/Edit Site Dialog Box	388
Site Links	392
Add/Edit Site Link Dialog Box	392
Site-to-Site Exclusions	392
Territories	393
Add/Edit Territory Dialog Box	393
Network Clouds	394
Add/Edit Network Cloud Dialog Box	394
Polycom CMA System Gatekeeper Functionality	394
Default, Redundant, Alternate, and Neighboring Gatekeepers	395
Default Gatekeeper	395
Redundant Gatekeeper	395
Alternate Gatekeeper	396
Neighboring Gatekeeper	396
Device Registration	396
Routing Mode	398
Direct Mode	398
Routed Mode	398
Polycom CMA System Integration with Microsoft Outlook	399
Standard Polycom CMA System and Reserved Conferencing	399
Polycom Conferencing for Microsoft Outlook, Reservationless Conferencing, and Calendaring Management	400
Polycom CMA System Integration with Microsoft Lync Server 2010 or Microsoft Office Communications Server 2007	401
Endpoint Directory and Directory Settings	401
 30 Server Setting Operations	403
Edit the Polycom CMA System Network Settings	403
Edit the Polycom CMA System Time Settings	404

Integrate with Microsoft Exchange Server for Calendaring Management . . .	405
Associate Sites with Microsoft Exchange Servers	405
Assign Calendaring Settings to Provisioning Profiles	406
Provision the Exchange Mailbox for Calendaring Service-enabled Endpoints	407
Integrate with Microsoft Lync Server 2010 or Microsoft Office Communications Server 2007	407
Provision Group for Microsoft Lync or Microsoft Office Communications Server Integration	408
Provision SIP Settings for Microsoft Lync or Microsoft Office Communications Server Integration	408
View Current Polycom CMA System Licensing	410
Add Polycom CMA System Licenses	411
Request a Software Activation Key Code	411
Enter the Polycom CMA System Activation Key	411
Reclaim Polycom CMA Desktop Licenses	412
Add or Remove a Polycom CMA System Custom Logo	412
Add or Remove a Polycom CMA Desktop Custom Logo	413
Edit the Polycom CMA System E-mail Account	414
31 Polycom CMA System SNMP	415
SNMP Overview	415
Polycom CMA System SNMP Operations	417
Enable SNMP Messaging	417
Edit the SNMP Settings for a Polycom CMA System	417
Add an SNMP Notification Receiver	419
Configure Alert Thresholds	421
Download Polycom CMA System MIB Package	422
Change the SNMP Communication Port	424
32 Database Operations	425
Overview of the Polycom CMA System Database	425
Internal Databases	426
External Databases	426
Database Restoration	427
Database Operations	427
Integrate a Polycom CMA System to an External Database	428
Revert a Polycom CMA System to its Internal Database	428
Copy the CMA System Database Backup Files	428
Reformat the Existing Database	429

33 Polycom CMA System Redundancy 431

Polycom CMA 5000 System Redundancy Overview	431
How Redundancy Works	431
Redundant Configuration System Administration	433
Implement a Redundant Polycom CMA 5000 System	434
Configure the External Database for Redundancy	435
Set the Virtual IP Address for the Redundant System	436
License a Redundant Polycom CMA System	437
Failover to a Redundant Polycom CMA 5000 System Server	437
Discontinue Redundancy on a Polycom CMA 5000 System Configuration .	438

34 Gatekeeper Management 439

Primary Gatekeeper Management Operations	439
Edit the Primary Gatekeeper Settings	439
Configure Prefixed Based Registration	441
Alternate Gatekeeper Management Operations	442
Add an Alternate Gatekeeper	442
Edit the Alternate Gatekeeper Settings	443
Remove the Alternate Gatekeeper	443
Neighboring Gatekeeper Management Operations	443
View Neighboring Gatekeepers	443
Add a Neighboring Gatekeeper	444
Edit a Neighboring Gatekeeper	444
Delete a Neighboring Gatekeeper	444

35 Management & Security Operations 445

Update the Polycom CMA System Software	445
Manage Certificates	446
Certificates Accepted by the Polycom CMA System	446
Certificate Operations	448
View Certificates and Certificate Details	448
Create a Certificate Signing Request	450
Install a Certificate	451
Upload a Certificate Revocation List	452
Delete a Certificate	453
View the Expiration Dates for Certificates and CRLs	454
Change the System User Interface Timeout and Number of Sessions ..	454
Give Enterprise Users Default Scheduler Role	455
Change the Message for Enterprise Users without a Role	455

Control Remote Desktop Connections to the CMA System	455
Automatic Registration Synchronization	456
Set Common Passwords for Endpoints	457
Disable Common Password for Endpoints	457
Set Local Account Lockout and Timeout	458
Set Local Password Requirements	458
Add Machine Accounts	460
Change Internal Database Passwords	461
36 Dial Plan Setup Operations	463
Site Operations	463
View the Graphical Site Topology	464
View the Sites List	464
Add a Site	465
View Site Information	473
Assign Locations to a Site	473
Edit Site Settings	475
Edit Site Provisioning Settings	475
Delete a Site	476
Set Up SIP	476
Edit SIP URI Data	477
Site Link Operations	478
View the Site Links List	479
Add a Site Link	479
Edit a Site Link	479
Delete a Site Link	480
Site-to-Site Exclusions	480
View the Site-to-Site Exclusion List	480
Add a Site-to-Site Exclusion	481
Edit a Site-to-Site Exclusion	481
Delete a Site-to-Site Exclusion	481
Territories	482
View the Territory List	482
Add a Territory	482
Edit a Territory	482
Delete a Territory	483
Network Clouds	483
View the List of Network Clouds	483
Add a Network Cloud	483
Edit a Network Cloud	484

Delete a Network Cloud	484
Dial Plan Service Operations	485
Conference on Demand	485
Simplified Dialing	486
View the Services List	490
Add a Service	490
Edit a Service	491
Delete a Service	491
Dial Rule Operations	492
Default Dial Rules	494
Parts of a Dial Rule	494
Pattern Types	494
Routing Actions	495
Examples of Custom Dial Rules	495
View the Dial Rules List	496
Add a Dial Rule	497
Enable or Disable Dialing Rules	497
Edit a Dial Rule	498
Least-Cost Routing Operations	498
How Least-Cost Routing Works	499
Example of Least-Cost Routing	499
LCR Tables for Three Sites	499
Call Scenario One	501
Call Scenario Two	501
Determining Area Codes	502
Determining Country Codes	502
Determining the Weighted Cost	502
View the Least Cost Routing Tables List	503
Add a Least Cost Routing Table	503
Edit a Least Cost Routing Table	503
Delete a Least Cost Routing Table	504
E.164 Numbering Scheme	504
E.164 Implementation in the CMA System	504
E.164 Alias Assignment	504
E.164 Numbering Scheme Default Settings	505
E.164 Numbering Scheme Explained	505
Generating E.164 Aliases	508
Setting-up an E.164 Alias in a User Dial String Reservation ...	508
Setting-up an E.164 Alias in a Room Dial String Reservation ..	509

37	Remote Alert Setup Operations	511
	Set Up Remote Alerts	511
	Set Up CMA System-generated E-mail Account	512
	Enable CMA System Remote Alerts	512
	Set CMA System Remote Alert Level Settings	513
	Set Endpoint Alert Level Settings	515
	Add a Remote Alert Profile	516
	Associate a Remote Alert Profile With a User	518
	Edit a Remote Alert Profile	519
	Disable a Remote Alert Profile	519
	Delete a Remote Alert Profile	519
	Disable CMA System Remote Alerts	520
38	System Management and Maintenance	521
	Management and Maintenance Overview	521
	Administrator Responsibilities	521
	Administrative Best Practices	522
	Auditor Responsibilities	522
	Auditor Best Practices	523
	Recommended Regular Maintenance	523
39	System Backup and Recovery Operations	525
	Backup Internal Databases and System Configuration	525
	Backup the CMA System Internal Databases	526
	Backup the CMA System Settings	526
	Restore Database and System Configuration	527
	Restore to Factory Default Image	527
	Restore from a Backup Archive	528
40	System Troubleshooting	529
	Troubleshooting Utilities Dashboard	529
	Troubleshooting Specific Types of Issues	531
	Registration Problems and Solutions	531
	Point-to-Point Calling Problems and Solutions	533
	MCU and Gateway Dialing Problems and Solutions	534
	Conference On Demand Problems and Solutions	535
	Gatekeeper Cause Codes	535

A	System Security and Port Usage	537
	Open Inbound Ports on the Polycom CMA System	537
	Outbound Ports Used by the Polycom CMA System	538

Polycom® CMA® System Overview

This chapter provides an overview of the Polycom® Converged Management Application™ (CMA®) system and includes these topics:

- [Polycom CMA System Features and Capabilities](#)
- [Polycom CMA System Models](#)
- [Minimum System Requirements](#)
- [Working in the Polycom CMA System](#)

Polycom CMA System Features and Capabilities

The CMA system is an integrated scheduling and device management platform for video conferencing that can include these features:

- The Polycom CMA Desktop client for Windows and MAC operating systems—an easy-to-use video and audio conferencing application that lets your users see and hear the people they call on their desktop system.
- Automatic provisioning for dynamically-managed endpoint systems and scheduled provisioning for standardly-managed and legacy endpoints.
- Automatic softupdates for dynamically-managed endpoint systems and scheduled softupdates for standardly-managed and legacy endpoints.
- On-demand conferencing using embedded MCUs or external MCUs.
- Conference scheduling via the CMA system Web Scheduler or the optional Polycom Scheduling Plugins for Microsoft® Outlook® or IBM® Lotus® Notes.®
- Advanced routing to distribute audio and video calls across multiple conferencing platforms (MCUs), creating a single seamless resource pool.
- Firewall management capabilities which enable videoconferencing across firewalls.
- Gatekeeper as well as alternate and neighboring gatekeeper functionality.

- Access to user and room directories for on-demand and scheduled calls. Directory services include:
 - Presence and contact list functionality for dynamically-managed endpoints.
 - Global Address Book for a single directory structure or Multiple Address Books for multiple managed directories.
 - H.350 and LDAP directory functionality. H.350 defines a directory services architecture for multimedia conferencing for H.323, H.320, SIP and generic protocols.
- Device monitoring and management.
- Conference monitoring and management.
- An optional high-availability, redundant management server configuration.

Polycom CMA System Models

Polycom offers two CMA system models.

- The single microprocessor CMA 4000 system supports up to 400 concurrently registered endpoints and 240 concurrent calls. Integration with a corporate directory and an external database is optional. The CMA 4000 system is not available in redundant configurations or maximum security configurations.
- The dual microprocessor CMA 5000 system can support up to 5000 concurrently registered endpoints and 3000 concurrent calls in direct mode and 1500 concurrent calls in routed mode. The CMA 5000 system is also available in an optional redundant configuration.

Integration with a corporate directory is optional for CMA 5000 systems. Integration with an external database (Microsoft SQL Server) is required for redundant CMA 5000 systems or for CMA 5000 systems supporting more than 400 concurrently registered endpoints and 240 concurrent calls.

Minimum System Requirements

The *Polycom CMA System Release Notes* describe the minimum system requirements for your CMA system. To find the most current *Release Notes*, go to support.polycom.com and navigate to **UC Infrastructure > Polycom Converged Management Application CMA 4000 & 5000**.

Any scheduled call that requires an external MCU requires a Polycom RMX™ or Polycom MGC™ conferencing platform. For example, any conference with a dial-in participant requires an external MCU. And some features and

services, such as Conference on Demand also requires an RMX or MGC system. Not all conferencing features are supported on all RMX system. For more information about supported functionality, see the *Polycom RMX System Release Notes* for your conferencing platform.

Working in the Polycom CMA System

This section includes some general information you should know when working in the CMA system. It includes these topics:

- [Log Into the Polycom CMA System](#)
- [Field Input Requirements](#)
- [Filter and Search a List](#)
- [Change a Password](#)
- [Log Out of the Polycom CMA System](#)
- [Restart or Shut Down a Polycom CMA System](#)
- [Emergency Shutdown of a Polycom CMA System](#)

Log Into the Polycom CMA System

To log into the CMA system web interface, you need:

- Microsoft Internet Explorer® 6.0, 7.0 or 8.0, Mozilla FireFox® 3.5 or 3.6, or Apple Safari 3.2, 4.0 or 5.0.

If your system is operating in maximum security mode, you may use only Microsoft Internet Explorer.

- Adobe® Flash® Player 9.x or 10.x
- The IP address or host name of the CMA system server and your username, password, and domain.



Note

The CMA system user interface is best viewed with an SXGA display resolution of at least 1280x1024 pixels. The minimum support display resolution is XGA 1024x768 pixels.

Generally, you get three opportunities to enter the correct password. After three failed attempts, the system returns an error message.

To log into a CMA system

- 1 Open a browser window and in the **Address** field enter the CMA system IP address or host name.
 - If prompted to install the Adobe Flash Player, click **OK**.
 - If you receive an **HTTPS Security Alert**, click **Yes**.
 - If you see a login banner, click **Accept** to accept the terms and continue.

If you cannot connect to the system, there may be certificate issues.

- 2 When the CMA system **Log In** screen appears, enter your **Username** and **Password**.
- 3 If necessary, select a different **Language** or **Domain**.
- 4 Click **Login**.

If you log in as an administrator, you see the CMA system **Dashboard**.

For more information about roles and the functionality associated with roles, see [“Default CMA System Roles and Permissions”](#) on page 253.

Field Input Requirements

While every effort was made to internationalize the CMA system, not all system fields accept Unicode entries. If you work in a language other than English, be aware that some CMA system fields may accept only ASCII or extended ASCII characters.

Filter and Search a List

In the CMA system interface, information is often summarized in lists or grids.

Lists that include many items may have filters or searchable fields, which allow you to view a subset of items or search for a specific entry. The available filtering options depend on the type of information in the list. For example in the conference list:

- If you select **Custom Date** as the filter, a calendar filter field appears.
- If you select **Ongoing Plus** as the filter, an attribute option appears. You can select the attribute **Conference Name** and enter all or part of the conference name into the associated text field.

In general, most text filter fields are ASCII only and the CMA system search function is a case-insensitive, substring search. That means when you enter a search string, the CMA system looks for that string wherever it occurs (beginning, middle, or end) in the word or number.

However, if the CMA system is integrated with an Active Directory, the CMA system uses the LDAP search function for searches of the directory. LDAP searches are prefix-searches that include an appended wildcard. In this case, when you enter a search string, the system looks for that search string only at the beginning of the indexed fields.

For example, all of the following searches for a participant will find Barbara Smithe:

Barbara
Smithe
Bar
Smi

To optimize LDAP searches, the CMA system (and its dynamically-managed endpoints) searches only indexed LDAP fields and a limited set of attributes.

The attributes include:

ObjectCategory
memberOf
DisplayName
GivenName
Sn
Cn
Samaccountname
groupType
distinguishedName
objectGuid

These are the requested attributes to be returned by the search:

Sn
Givename
Mail
Ou
Objectguid
Telephonenumber
Cn
Samaccountname
Memberof
Displayname
Objectclass
Title
localityName
department

Change a Password

For local users, CMA system password requirements (for example, password length and password age) are managed by the CMA system administrator. For enterprise users, CMA system password requirements are managed by Microsoft Active Directory.

To change your system password

- 1 Click **Settings** in the top-right corner of the page.
- 2 In the Settings dialog box, click **Change Password**.
- 3 Enter your **Old Password**.
- 4 Enter a **New Password**.
- 5 Confirm the new password and click **OK**.

Log Out of the Polycom CMA System

To log out of the CMA system

- Click **Log Out** in the top-right corner of the page.

Restart or Shut Down a Polycom CMA System

You have several options for an orderly shutdown or restart of a CMA system in non-emergency situations.



The options for an orderly shutdown or restart of the system include:

- Use the **Shutdown** option on the user interface when you must disconnect the CMA system server for some reason; for example, to move it. All CMA system functionality is stopped during a **Shutdown**.
- If the system interface is not available and you must shut down the system, press once (but do not hold) the power switch on the CMA system server. This is equivalent to selecting the **Shutdown** option described previously.
- Use the **Restart** option on the user interface when you must cycle the CMA system for some reason; for example, if the system locks up or loses connection with the database.

If you have access to the CMA system user interface, you can also stop future scheduled conferences from starting automatically and wait for active conferences to end before performing an orderly shut down or restart of the system.

During a restart, the system will drop all IP conferences. In general, ISDN conferences will not drop. Also, endpoints registered to the gatekeeper will drop. IP endpoints not registered with the gatekeeper can continue in conference.

To restart or shut down a CMA system

- 1 (Optional) To stop future scheduled conferences from starting before you perform the restart or shutdown:
 - a Go to **Admin > Conference Settings**.
 - b Check the **Conference Auto-Launch Disabled** check box and click **Update**.
 - c Go to **Admin > Dashboard**.
 - d Monitor the **Today's Conferences** section to determine when all active conferences are completed.
- 2 Go to **Admin > Dashboard** and click **Restart**  or **Shutdown** , as required.

In a redundant CMA system configuration, if you requested a shutdown of the primary server, the system displays a warning indicating that it is initiating a failover.

If you select **Restart**, it may take the CMA system up to 10 minutes to shutdown and then restart all server processes.

Emergency Shutdown of a Polycom CMA System

You have two options to perform an emergency shutdown of a CMA system. Use these options only when you must immediately cut power to the server.

- Press and hold the power switch on the CMA system server.
- Pull the system power cord.

After an emergency shutdown (that is when you press and hold the power switch, or you pull the system cord, or you lose power to the system), a system battery may continue to cache information until the battery runs out. In this case, the system enters an error state. To recover, you must connect a keyboard and monitor to the CMA system and boot the system to clear the error message. Then the system can begin recovery.

Polycom CMA System Configuration

This chapter describes the configuration tasks that may be required, based on your system design and installation to complete your implementation of a Polycom® Converged Management Application™ (CMA®) system after **First Time Setup**. It includes these topics:

- [Add DNS SRV Record for Polycom CMA System Services](#)
- [Configure the Connection to the External Database](#)
- [Configure the Connection to an External Enterprise Directory](#)
- [Configure Redundancy](#)
- [Set Up Video Call Routing](#)
- [Set Up Automatic Provisioning](#)
- [Set Up Automatic Softupdate](#)
- [Set Up Conference Templates](#)
- [Set Up Directory Services](#)
- [Set Up a Certificate for the Polycom CMA System](#)
- [Distribute Polycom Applications](#)



IMPORTANT

If during **First Time Setup**, you enabled the **Maximum Security** option, please see [“Operating in Maximum Security Environments”](#) on page 17 for information about how the system operates in this configuration.

Add DNS SRV Record for Polycom CMA System Services

You must configure the DNS server, if you wish it to resolve queries for the CMA system by the CMA system’s host name or IP address.

We recommend that the DNS server be configured to find the CMA system by its fully qualified domain name (FQDN). This ensures that client systems running desktop Polycom CMA Desktop can access the CMA system.

The DNS should also have entries for your Active Directory server (if different from the DNS) and for the external database server being used by the CMA system.

**Note**

If you configure the DNS server to use two or more Active Directory servers, make sure that the servers have the same services available.

To dynamically manage endpoints (which includes automatic provisioning, automatic softupdate, and presence) right out-of-the-box, they must be able to automatically discover the CMA system. This means you must add the DNS service record (SRV record) for the CMA system. The lookup key for this service record is `_cmaconfig._tcp`. So the record will resemble this:

```
__cmaconfig._tcp.customerdomain.com 86400 IN SRV 0 0 443 cma5000.customerdomain.com
```

For more information about DNS, DNS records, and how DNS works, see Microsoft Technet

([http://technet.microsoft.com/en-us/library/cc772774\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc772774(WS.10).aspx)).

Configure the Connection to the External Database

If during **First Time Setup** you did not configure the CMA system to use an external Microsoft SQL Server database, but need to do so now, see “[Database Operations](#)” on page 427.

**Note**

It is not recommended, but you can create the CMA system databases manually using Microsoft SQL scripts. Contact Polycom Global Services to request the creation scripts.

Integration with an external Microsoft SQL Server database is required for redundant CMA 5000 systems or for CMA 5000 systems supporting more than 400 concurrently registered endpoints and 240 concurrent calls.

Configure the Connection to an External Enterprise Directory

If during **First Time Setup** you did not configure your CMA system to use an enterprise directory, but need to do so now, see “[Directory Operations](#)” on page 355.

Connecting to an enterprise directory allows users to enter their network usernames and password to log into CMA system. It also allows users to access the enterprise directory when selecting conference participants.

Configure Redundancy

You can install the CMA 5000 system in a fault-tolerant, high-availability, redundant configuration. The CMA 4000 system is not available in a redundant configuration.

A redundant CMA system configuration requires the installation of two CMA system servers on the same network. During **First Time Setup**, you are instructed to assign these two servers physical IP addresses. Once the two system servers are installed, see [“Polycom CMA System Redundancy”](#) on page 431 to finish implementing redundancy.

Set Up Video Call Routing

The video call routing setup includes the gatekeeper, site topology, gateway and MCU dial plan services, and bandwidth management.

You can perform the following tasks:

- Handle inbound ISDN calls and route them to correct endpoints.
- Enable outbound IP- based calls.
- Connect through a firewall using an SBC device.
- Allow or deny calls to and from unregistered endpoints (rogue calls).
- When you have a third-party MCU that registers with the gatekeeper using standard H.323 protocol, add gateway and MCU dial plan services manually.
- Define new sites and site links.
- Add IP-to-ISDN call routing using least-cost routing.
- Define neighboring gatekeepers.
- Enable routing of H.323 calls to neighboring gatekeepers.
- Define a site for each physical location in which a LAN or an ISDN connection exists. If you use VPN connections, you can consolidate distinct physical locations into a single logical site to simplify management tasks.
- For each site, define the subnets in which the video endpoint systems are deployed. It is important that the IP addresses used by the endpoints belong to only one subnet at a site.
- Define least-cost routing tables only when you use the least-cost routing feature.
- Customize default dialing rules.

For more information, see [“Dial Plan Setup Operations”](#) on page 463.

Set Up Automatic Provisioning

The CMA system automatic provisioning feature allows an administrator to configure one or more endpoints with the standard set of information the registering endpoints need to operate within the network. This eliminates the need to configure each endpoint individually.

Automatic provisioning is enabled at the endpoint, but the CMA system must have automatic provisioning profiles for both the endpoint and the site at which the endpoint resides.

To ensure out-of-box usability, the CMA system comes with default automatic provisioning profiles. However, to create your desired user experiences, you should:

- Create customized automatic provisioning profiles for endpoint types.
- Edit provisioning profile for each site.

For more information, see [“Automatic Provisioning Operations”](#) on page 183.

Set Up Automatic Softupdate

The CMA system automatic softupdate feature allows an administrator to upgrade the software on one or more endpoints with a standard software package. This eliminates the need to upgrade each endpoint individually.

The automatic softupdate feature is enabled at the endpoint. At start up and at designated intervals, endpoints in automatic softupdate mode automatically look for a new softupdate profile and package on the CMA system.

To implement automatic softupdates, you must create a softupdate package for each endpoint type you wish to support with updates.

For more information, see [“Automatic Software Update Operations”](#) on page 191.

Set Up Conference Templates

The CMA system uses conference templates and global conference settings to manage system and conference behavior.

The CMA system has a **Default Template** and default global conference settings. You may want to create additional templates with different settings or change the global conference settings.

For more information, see [“Polycom® CMA® System Conference Scheduling Overview”](#) on page 39.

Set Up Directory Services

Directory services provide information about all users, endpoints, and resources on your video communication network.

To set up CMA system directory services, complete the following tasks:

- 1 Register devices. On endpoints, you must set the gatekeeper and/or Global Directory Server (GDS) to point to the CMA system IP address or DNS name. We recommend using the IP address to prevent data inconsistencies.

It may take a device up to 5 minutes to register with the gatekeeper and indicate an online status.

Most device information is automatically populated in the CMA system through the gatekeeper registration or Global Address Book access. You must review the information for these devices in the CMA system **Directory Setup** page and fill in missing information.

To select endpoints when scheduling conferences, you must first associate them with a user or conference room by editing the specific user or room settings. For more information, see [“Endpoint and Peripheral Management Operations”](#) on page 165.

- 2 Set up users and associate them with endpoints. Unless your CMA system is integrated with an enterprise directory, you must enter all user information manually including endpoint association. If your system is integrated with an enterprise directory, general user information (**First Name, Last Name, UserID, Password, E-mail Address**) is directly pulled from the directory and cannot be changed. However, you must still associate enterprise users with endpoints. For more information, see [“Users and Groups Overview”](#) on page 249.
- 3 Set up groups, add members, and associate them with provisioning profiles. For more information, see [“Users and Groups Overview”](#) on page 249.
- 4 Set up rooms and associate them with endpoints. Unless your CMA system is integrated with an enterprise directory that includes conference rooms, you must enter all room information manually including endpoint association. For more information, see [“Room Overview and Operations”](#) on page 343.

Set Up a Certificate for the Polycom CMA System

By default, the CMA system uses *https* and a self-signed certificate for its data interchanges. As a best practice, we recommend replacing the CMA system self-signed certificate with a certificate from a Certificate Authority. For more information, see [“Manage Certificates”](#) on page 446.

Distribute Polycom Applications

The CMA system allows you to download several Polycom applications for use in specific environments. This includes two scheduling plugins and two desktop video applications. These are:

- [Distribute Polycom CMA Desktop for Windows Systems](#)
- [Distribute Polycom CMA Desktop for MAC OS Systems](#)

These are discussed in the following topics.



Note

- The Polycom RealPresence Desktop can be downloaded from the Polycom website at support.polycom.com.
- The Polycom RealPresence Mobile application for Android™ can be downloaded from play.google.com/store.
- The Polycom RealPresence Mobile application for iPhone® and iPad® can be downloaded from the www.apple.com/store.

Distribute Polycom CMA Desktop for Windows Systems



IMPORTANT

- On a Windows XP system, the user installing the Polycom CMA Desktop must sign in with administrative privileges. On a Windows Vista system, the user installing the Polycom CMA Desktop must sign into the **Administrator** account.
- The following procedures assumes you have implemented DNS lookup and Windows authentication for single sign on.

To deploy the CMA Desktop client to users, you have at least four distribution options

Option 1: Distribute the CMA Desktop client via an E-mail link

You can copy the link for the **CMA Desktop** client from the CMA system **Downloads** page into an E-mail that you can send to users.

To do this, copy and paste the CMA Desktop link (for example, *http://10.47.9.136/SoftUpdate/vv1/CMADesktop_4_1_1_1010/CMADesktop.exe*) from the **Downloads** page into an E-mail to be sent to users. Include the IP address of the CMA system and usernames and passwords (as required) in the E-mail to users.

Option 2: Distribute the CMA Desktop client via the management system

You can provide users access to the CMA system, from which they can download the CMA Desktop client.

To do this, copy and paste the IP address of the CMA system into an E-mail to be sent to users. Include usernames and passwords (as required) in the E-mail to users and instruct them to access the **Downloads** link.

Option 3: Distribute the CMA Desktop client via a desktop management or group policy object

Distribute the **.exe** installation file as a desktop management or group policy object to a location on client systems and provide directions to users on how to run the executable.

To do this, build a desktop management or group policy object that writes the **.exe** installation file to a directory (for example, *C:\temp*) on the user's local system. Include the command for executing the file in an E-mail to be sent to users. For example:

```
C:\temp\CMA Desktop.exe"/s /v"/qn SBSERVERTYPE=2 SBSERVERADDRESS=nnn.nnn.nnn.nnn
```

Include the IP address of the CMA system and usernames and passwords (as required) in the E-mail to users.

Option 4: Distribute the CMA Desktop client via a .zip file

Zip the **.exe** installation file and send it in an E-mail to users. Include the IP address of the CMA system and usernames and passwords (as required) in the E-mail to users. For endpoints on the public network that will be accessing the system through a firewall, include the IP address of the Polycom VBP system rather than the CMA system.

Distribute Polycom CMA Desktop for MAC OS Systems



IMPORTANT

- On a MAC system, the user installing the CMA Desktop client must sign in with administrative privileges and an **Administrator** account.
- The following procedures assumes you have implemented DNS lookup and MAC authentication for single sign on.

To deploy the CMA Desktop for MAC OS clients to users, you have at least three distribution options

Option 1: Distribute the CMA Desktop for MAC OS client via an E-mail link

You can copy the link for the CMA Desktop for MAC OS clients from the CMA system **Downloads** page into an E-mail that you can send to users. To do this, copy and paste the CMA Desktop for MAC OS link (e.g., http://10.47.9.136/SoftUpdate/vv1/CMADesktopMac_5_1_0_7458/CMADesktop.dmg) from the **Downloads** page into an E-mail to be sent to users. Include the IP address of the CMA system and usernames and passwords (as required) in the E-mail to users.

Option 2: Distribute the CMA Desktop Mac client via the management system

You can provide users access to the CMA system, from which they can download the client. To do this, copy and paste the IP address of the CMA Desktop Mac system into an E-mail to be sent to users. Include usernames and passwords (as required) in the E-mail to users and instruct them to access the Downloads link.

Option 3: Distribute the CMA Desktop Mac client via a .dmg file

Send the *.dmg* file in an E-mail to users. Include the IP address of the CMA system and usernames and passwords (as required) in the E-mail to users. For endpoints on the public network that will be accessing the system through a firewall, include the IP address of the Polycom VBP system rather than the CMA system.

Operating in Maximum Security Environments

This chapter describes how the Polycom® Converged Management Application™ (CMA®) system operates when in Maximum Security mode. It includes these topics:

- [Maximum Security Mode Overview](#)
- [Conference Scheduling in Maximum Security Mode](#)
- [Endpoint Management in Maximum Security Mode](#)
- [Network Device Management in Maximum Security Mode](#)
- [User Management in Maximum Security Mode](#)
- [Group Management in Maximum Security Mode](#)
- [Reporting in Maximum Security Mode](#)
- [Device Administration in Maximum Security Mode](#)
- [System Administration in Maximum Security Mode](#)
- [Network Intrusion Detection in Maximum Security Mode](#)
- [Troubleshooting in Maximum Security Mode](#)

Maximum Security Mode Overview

The CMA system provides a **Maximum Security** option for those businesses that must adhere to the most stringent security protocols.

You can only enable the **Maximum Security** option during **First Time Setup**. The process is irreversible and has significant consequences, as many CMA system features aren't supported in this mode.

- In maximum security, the CMA system does not include support for the following features:
 - Operation on the CMA 4000 platform or in a redundant system configuration
 - CMA system gatekeeper functionality
 - External databases
 - Legacy endpoints. Only HDX systems operating in dynamic management mode are supported.
 - ISDN scheduling
 - Global Address Books
 - Standard (scheduled) management and monitoring of endpoints
 - Presence
 - SNMP
 - Remote desktop
 - Integration with Microsoft (MS) Exchange for calendaring
 - Integration with MS Office Communications Server or MS Lync
 - Support for the Polycom CMA Desktop clients or the Polycom Scheduling Plug-ins for Microsoft Outlook and IBM Lotus Notes
 - Least Cost Routing
 - Audio only conferences
 - Online help

The following sections describe in detail the operational differences for a CMA system in Maximum Security mode.

Conference Scheduling in Maximum Security Mode

Conference scheduling functionality is available to users assigned the basic **Scheduler**, **Advanced Scheduler**, and **Operator** roles. The conference scheduling workflow on a CMA system operating in maximum security mode does not change. However, because all conferences must be hosted on RMX conferencing systems, the **MCU Settings** for all **Conference Templates** has changed in the following ways:


- The **Supported MCUs** section lists only **RMX** systems.
- The **Always Use MCU** option on the **Conference Template** page is not available (grayed-out); it is always enabled and cannot be changed.

Endpoint Management in Maximum Security Mode



Endpoint management functionality is available to users assigned the **Device Administrator** role. Users assigned the standard **Administrator** role may only monitor endpoints.

The endpoint management workflow on a CMA system operating in maximum security mode changes in that it only supports HDX endpoints operating in dynamic management mode. The system changes made to support this workflow change include:

- The **Scheduled Provisioning** and **Scheduled Software Update** pages and the **ACTIONS** associated with them are not available.
- Only HDX endpoints that are automatically provisioned by the CMA system are displayed in the endpoint list.
- The **ACTIONS** on the **Endpoint > Monitor View** page changes as follows:

Actions	Use this action to...
Add 	Not available. Endpoints can only be added to the system during automatic provisioning.
Search Devices	Not available.

- The **Device Summary** section of the **Endpoint > Monitor View** page does not change.
- The **Device Status** section of the **Endpoint > Monitor View** page changes as follows:

Field	Description
Gatekeeper Registration	The status of the device's registration with the gatekeeper service always indicates  Unknown .
Directory Registration	The status of the device's registration with the Global Directory Service always indicates  Not Registered .
Presence Registration	Not available.
Exchange Registration	Not available.
SIP Registration	Not available.
Device Managed	Indicates Heartbeat Timeout .
Gatekeeper Address	The IP address of the gatekeeper to which the device is registered.
Last GK Registration	Not available.

Field	Description
ISDN Line Status Type	Not available.
ISDN Assignment Type	How the ISDN type was assigned to the device. This always indicates Undefined .
Device ISDN Type	Not available.

- The **Call Info** section of the **Endpoint > Monitor View** page does not change.
- The **Device Alerts** section of the **Endpoint > Monitor View** page changes as follows:

Field	Description
Errors	Device error message text always shows Gatekeeper Unregistered .

- The **Provisioning Details** section of the **Endpoint > Monitor View** page does not change.

Network Device Management in Maximum Security Mode

Network device management functionality is available to users assigned the **Device Administrator** role. Users assigned the standard **Administrator** role may only monitor network devices.

The network device management workflow on a CMA system operating in maximum security mode changes in that it supports only RMX conferencing systems. The system changes required for this workflow change include:

- The **VBP**s and **DMA**s pages and the **ACTIONS** associated with them are not available.
- The **ACTIONS** on the **MCU > Monitor View** page do not change.
- The **Add New Device** dialog box for the RMX MCU does not change. Note that when operating in maximum security mode, the **Admin ID** for an MCU is the CMA machine account created on the RMX system just for this purpose and the **Password** is the password designated for this CMA machine account.

Polycom RMX Systems in Secure Mode

The CMA system automatically detects when a Polycom RMX system is operating in secure (HTTPS) mode. By default, in non-secure (HTTP) mode, the Polycom RMX system uses port 80 for its communications and in secure (HTTPS) mode, the Polycom RMX system uses port 443 for its communications.

You can determine via the CMA system interface whether or not a Polycom RMX system is operating in secure mode by viewing the HTTP port number for the MCU (see [“View Device Details”](#) on page 227).

If an administrator changes the secure mode setting on a Polycom RMX system, the CMA system will lose connection to the RMX, but will automatically regain it using the correct protocol. The CMA system may take up to a minute to restore the connection.

User Management in Maximum Security Mode

User management functionality is divided among different roles: **Scheduler**, **Operator**, and **Administrator**.

Scheduler

Users assigned the basic **Scheduler** and **Advanced Scheduler** role can add guest participants to the **Guest Book**.

The **Guest Book** workflow for schedulers on a CMA system operating in maximum security mode has not changed.

Operator

Users assigned the **Operator** role can add, edit, and delete guest participants from the **Guest Book** as well as add, edit, and delete their own **Favorites** lists.

The **Guest Book** and **Favorites** workflow for operators on a CMA system operating in maximum security mode has not changed.

Administrator

The administrator’s user management functionality and workflow on a CMA system operating in maximum security mode has changed significantly.

When integrated with an enterprise directory (Microsoft Active Directory), the CMA system can have only one local account – the default administrator account used to access and administer the system. This account cannot be deleted in any circumstances.

When integrated with an enterprise directory, this local administrator can perform the following user management functions:

- Integrate the CMA system with Active Directory. Note that when you integrate the CMA system with an Active Directory, all local users other than the default local administrator are removed from the system.
- Edit a subset of enterprise user attributes, such as their role, area, or endpoint associations. This allows the local administrator to assign the **Administrator** role to enterprise users.
- Troubleshoot and administrate the system if the Active Directory connection to the system is lost.

When not integrated with an enterprise directory, this local administrator can perform the following user management functions:

- Add and edit local user attributes including their contact information and other user attributes such as their role, area, or endpoint associations.
- Delete local users.



Note

As a best practice, use this local administrator account for user management tasks on the CMA system. Do not use it to log into managed devices.

The user management workflow on a CMA system operating in maximum security mode has changed in the following ways:

- Once integrated with an enterprise directory, the local administrator can see enterprise users as well as associate them to endpoints, roles, and areas (when applicable).
- Administrators cannot create custom roles with a custom set of permissions. The system has only pre-defined roles and associated permissions as described in [“Default CMA System Roles and Permissions”](#) on page 253.

The system changes required to support this workflow change are:

- The **User Roles** page and the **ACTIONS** associated with it are not available.
- The **ACTIONS** on the **User > Users** page includes an additional command, so that you can view the permissions that come with the role a user has been assigned.

Action	Use this action to...
View Permissions	Display the set of permissions that come with the user's assigned role.

- Administrators cannot assign users more than one role.

The system change required to support this workflow change is:

The user interface for assigning roles (**Add/Edit User > Associated Roles**) has changed to a radio button list from which you can assign only one role from a set of mutually exclusive, predefined options.

- Via the **Edit** function, local administrators can now enable and disable local users rather than permanently deleting their user accounts. This function is only available for local users. Enterprise users must be enabled and disabled in Active Directory.



Note

Disabled local users (when not integrated with an enterprise directory) still appear in the CMA system **Users** list. However, disabled enterprise users (when integrated with an enterprise directory) won't appear in the CMA system **User** list if the **Ignore Disabled Enterprise Directory Users** option on the **Enterprise Directory** page is enabled.

The system change required to support this workflow change is:

The **General Info** tab of the **Edit User** dialog box now has an **Enable User** option. By default, when a local user is created, this option is selected.

- Via the **Edit** function, administrators can unlock user accounts that become locked when a user reaches the **Failed login threshold**.



Note

Administrators cannot lock user accounts. This functionality is triggered only when the failed login threshold is met.

The system change required to support this workflow change is:

The **General Info** tab of the **Edit User** dialog box now has an **Unlock User** option. By default, when a local user is created, this option is not selected. However, when a local user reaches the **Failed login threshold**, the administrator can reset the lock by enabling the **Unlock User** option.

- Users cannot be associated with an alert profile because a CMA system operating in maximum security mode does not include remote alerts.

The system change required to support this workflow change is:

The **Add/Edit User > Associated Alert Profile** tab has been removed from the user interface.

A CMA system has password requirements, local user account configuration requirements, and session management requirements that affect local users and local user accounts. For more information about these requirements, see [“Management and Security”](#) on page 30.

Group Management in Maximum Security Mode

Group management functionality is available to users assigned the **Administrator** role.

The group management workflow on a CMA system operating in maximum security mode has not changed except that users cannot inherit roles from groups.

When not integrated with an enterprise directory, local administrators can add local groups with local users. When integrated with an enterprise directory, the single local administrator and any enterprise users assigned the **Administrator** role can **Add** local groups, **Import Enterprise Groups**, and **Synchronize Groups** with Active Directory.

Reporting in Maximum Security Mode

Reporting functionality is divided among different roles: **Administrator**, **Operator**, and **Auditor**.

Administrator

The administrator's reporting functionality and workflow on a CMA system operating in maximum security mode has changed. Users assigned the **Administrator** role can access the following system reports:

- Endpoint Usage Report
- Conference Type Report
- System Log Files
- Audit Log Files

Users assigned the **Administrator** role cannot access the following system reports, since these reports have been removed from the system:

- Site Statistics
- Site-link Statistics
- IP Call Detail Records
- Conference Usage Report
- Gatekeeper Message Log

For more information on these reports, see [“System Reports”](#) on page 281.

Operator

The operator's reporting functionality and workflow on a CMA system operating in maximum security mode has changed. Users assigned the **Operator** role can only access the following system report:

- Conference Usage Report

Users assigned the **Operator** role cannot access the following system reports:

- IP Call Detail Records
- Endpoint Usage Report
- Gatekeeper Message Log

For more information on these reports, see the *Polycom CMA System Administrator's Guide*.

Auditor

Users assigned the **Auditor** role can access the following system reports:

- Endpoint Usage Report
- System Log Files
- Audit Log Files

For more information on these reports, see the *Polycom CMA System Administrator's Guide*.

The **Auditor** role and workflow allows the auditor to:

- View online the **Endpoint Usage Report** for selected endpoints.

The system change required to support this workflow change is:

The **Endpoint Usage Report** menu option and page is available from the **Reports** menu, but the **Generate Report** and **Download All CDRs** options are not available to the auditor.

- Download the **System Log Files**.

The system changes required to support this workflow change are:

- The **System Log Files** menu option and page is available from the **Reports** menu.
- The **Download ALL** command is available from the list of **ACTIONS**.

- **Backup and Delete** audit log files.

The system changes required to support this workflow change are:

- The **Audit Log Files** menu option and page is available from the **Reports** menu.
- The **Backup and Delete** command is available from the list of **ACTIONS**. This option allows an auditor to backup and delete selected audit logs. During this process, the CMA system requires that

the auditor download and run a verification utility that performs a checksum operation to make certain that the downloaded audit log is complete and uncorrupted before the audit log is deleted from the CMA system.

- Change the audit log **Alert Level**.

The system change required to support this workflow change is: The **Change Settings** command is available from the list of **ACTIONS**. By default the audit log **Alert Level** is set to 70% of the **Max File Size Usage**, which is 2 gigabytes.

Device Administration in Maximum Security Mode

Only users assigned the **Device Administrator** role can perform device administration tasks.

In addition to the tasks described in the [Endpoint Management in Maximum Security Mode](#) section, the device administrator workflow on a CMA system operating in maximum security mode allows the device administrator to:

- See the system **Dashboard**.
- Add, edit, and delete machine accounts for endpoint systems.

The system change required to support this workflow change is: The **Machine Accounts** menu option and page is available from the **Admin > Management and Security** menu. Before the CMA system can dynamically manage a HDX system, a device administrator must add a machine account for the HDX system. This is the same username that the HDX system administrator should enter on the HDX system for the provisioning service. This allows the HDX and CMA systems to authenticate and communicate without using a specific user's account.

About Machine Accounts

Before the CMA system can dynamically manage HDX systems operating in maximum security mode, a user assigned the **Device Administrator** role must create an HDX machine account for each HDX that the CMA system will manage. The machine account allows the endpoint to connect and authenticate with the CMA system for dynamic management purposes without using the endpoint user's account.

The **Add Machine Account** dialog box includes the following information.

Field	Description
Enable Machine Account	Select or clear this option to enable and disable (respectively) the machine account you create for the endpoint.

Field	Description
Unlock Machine Account	Select this option to unlock machine accounts that become locked when they exceed the Failed login threshold. This will only happen when the password expires.
User ID	Enter a unique name for the machine account. As a best practice, name the machine account in a way that associates it with the corresponding device. For example, if your company names endpoint systems for the system user or room (for example, <i>bsmith_HDX</i> or <i>Evergreen_Room</i>), then give the machine account an associated User ID (<i>bsmith_HDX_machine</i> or <i>evergreen_room_machine</i>).
Password/ Confirm Password	Enter a password for the machine account user ID. This password must meet the Local Password Requirements . This password expires in 365 days.
Description	Enter a meaningful description for the endpoint.
Associate with an existing user or room	Select this option to associate the endpoint system with a specific user or room. This may be a local or enterprise user or room.
Associate with a new room (created automatically)	Select this option to associate the endpoint system with a system-generated room name.

Once you have created this machine account on the CMA system, provide this information to the appropriate HDX system administrator. They should enter this **User ID** and **Password** as the **User Name** and **Password** on the HDX **Provisioning Service** page.

Note that the machine account password expires after one year. After the expiration, the HDX login will fail. After three failed login attempts, the system locks the machine account. You can reset the password and unlock the machine account by editing it and assigning a new password.

System Administration in Maximum Security Mode

Only users assigned the **Administrator** role can perform general CMA system administration functions. The CMA system administration functionality and workflow on a CMA system operating in maximum security mode has changed. The following sections describe the areas of functionality and how they have changed.

Users assigned the **Administrator** role can see the system **Dashboard**, the **Admin** menu, and the pages and **ACTIONS** associated with it.

Admin Menu

The **Admin** menu in maximum security mode changes in the following ways:

- The **Global Address Book**, **SNMP Settings**, **Gatekeeper Settings**, and **Alert Settings** menu options and their associated functionality have been removed.
- Removed gatekeeper functionality resulted in the following system changes:
 - The system cannot display bandwidth usage. Bandwidth usage for sites, subnets, or site limits is always 0.
 - Site exclusions cannot be enforced.
 - Dial rules are required for ISDN calling in translating numbers, but have no affect for IP calls.
 - The system is not the gatekeeper, so it cannot perform address resolution.
 - E164 aliases assigned by the CMA system are not communicated to the gatekeeper, so they cannot be resolved.
 - Dialing rules can be configured on the CMA system, but they are not communicated to the gatekeeper, so they cannot be implemented.
 - Threshold alarms and hardware alarms are always 0.
 - Site topology cannot provide a graphical representation of status (color).
 - The CMA system has no knowledge of external gatekeeper or its rules.

Conference Templates

As was noted before, because all conferences scheduled on a CMA system operating in maximum security mode must be hosted on a RMX conferencing system, the **MCU Settings** for all **Conference Templates** has changed in the following ways:

- The **Supported MCUs** section lists only **RMX**.
- The **Always Use MCU** option on the **Conference Template** page is not available (grayed-out); it is always enabled and cannot be changed.

Conference Settings

On a CMA system operating in maximum security mode, a setting is available on the **Conference Setting** page. The **Conference and chairperson password length** field allows an administrator to designate the required length of the system-generated conference password and chairperson password. The acceptable length for both of these passwords is six to 16 characters. By default, the required length for both of these passwords is set to 15 characters.

**Note**

Depending on the system settings, the scheduler may be allowed to change the Conference Password or Chairperson Password. However, the password length requirement still applies.

Other than this requirement, the conference settings, conference password, and chairperson password workflow on a CMA system operating in maximum security mode have not changed.

Provisioning Profiles

Because a CMA system operating in maximum security mode supports only HDX endpoints running version 2.7.0J operating in dynamic management mode, the **Scheduled Provisioning Profiles** page and the **ACTIONS** associated with it are not available.

The **Automatic Provisioning Profiles** page and the **ACTIONS** associated with it has not changed on a CMA system operating in maximum security mode.

Software Updates

Because a CMA system operating in maximum security mode supports only HDX endpoints running version 2.7.0J operating in dynamic management mode, the **Scheduled Software Update** page and the **ACTIONS** associated with it are not available.

The **Automatic Software Update** page and the **ACTIONS** associated with it has not changed on a CMA system operating in maximum security mode.

Server Settings

The **Server Settings** menu for a CMA system operating in maximum security mode has changed significantly. The following options have been removed:

- Database
- Calendaring Management
- Microsoft Lync or Office Communications Server Integration
- Redundant Configuration
- Remote Alert Setup
- E-mail

In addition, you will also note the following changes and additions:

- The **Network** settings page now includes the ability to enable IPv6 and to include a preferred and alternate DNS server.

- The **System Time** page does not include the **Minutes Between Synchronization** option when using an NTP server.
- What was formerly titled the **LDAP** page is now titled the **Enterprise Directory** page.
- On the **Enterprise Directory** page:
 - You must identify the enterprise directory by **DNS Name**. You cannot identify the enterprise directory server by IP address.
 - The **Security Level** defaults to StartTLS and cannot be modified.
- The **Reclaim Inactive CMA Desktop Licenses** option has been removed from the **Licenses** page.
- The **CMA Desktop Logo** option has been removed from the **Custom Logo** page.
- The **Include dynamically-managed devices in the Global Address Book** option has been removed from the **Directory Setup** page.

Management and Security

A CMA system operating in maximum security mode offers a **Management and Security** workflow. The following sections describe the changes.

Server Software Upgrade

The **Server Software Upgrade** workflow on a CMA system operating in maximum security mode has not changed.

Certificate Management

Because a CMA system operating in maximum security mode always operates in encrypted mode, the **Use HTTPS** is not an option on the Certificate Management page.

By default, to support encrypted communications and establish a minimum level of trust, the CMA system includes a default key and self-signed certificate. However, to implement a full certificate chain to a root certificate authority (CA), a CMA system requires both a root CA certificate and a identity server certificate signed by the root CA. Therefore, at some time you must request these certificates from your CA. The question is when.

You must install the root CA certificate during First Time Setup. However, you can complete First Time Setup with just the root CA certificate and the CMA system default self-signed certificate. Then you can use the Certificate Management page to finish certificate set up.

Session Management

The **Session Management** page allows an administrator to change but not disable the following settings:

Field	Description
CMA user interface timeout	By default the CMA system user interface times out after 10 minutes of inactivity. Use this procedure to change the timeout value for the user interface inactivity timer. Possible value is 5 to 60 minutes.
Maximum number of sessions per user	The number of simultaneous login sessions per user ID. Possible value is 1 to 10 sessions.
Maximum number of sessions per system	<p>The number of simultaneous login sessions by all users. Possible value is 2 to 50 sessions.</p> <p>Note</p> <p>If this limit is reached, but none of the logged-in users is an Administrator, the first Administrator user to arrive is granted access, and the system terminates the non-Administrator session that's been idle the longest.</p>

Banner Configuration

The **Banner Configuration** page allows users assigned the **Administrator** role to customize (but not disable) the long and short login banners.

A log in banner is the message that appears when users attempt to access the system. Users must acknowledge the message before they can log in.

By default, the long banner field on the **Banner Configuration** page displays the required Standard Mandatory Notice and Consent Provision for systems operating in maximum security mode. The short banner field displays a shortened version of this same notice.

The long banner is used for the CMA system log in banner. It is also provisioned to HDX systems that the CMA system manages. The short banner is provisioned to HDX systems that the CMA system manages for those situations in which the long banner length exceeds the available display area.

The CMA system provides several sample long banners. You can use these banners as is or edit them to create a custom long banner. The CMA system provides a single short banner, which you can also customize. If you customize the banners, remember that the long banner message may contain up to 5000 characters. The short banner message may contain up to 1315 characters.

Local User Account Management

The **Local User Account Management** page allows an administrator to change but not disable the following local user account settings:

Field	Description
Account Lockout	
Failed login threshold	Specify how many consecutive login failures cause the system to lock an account. Possible value is 2 to 10.
Failed login window (hours)	Specify the time span within which the consecutive failures must occur in order to lock the account. Possible value is 1 to 24.
Customized user account lockout duration (minutes)	Specify how long the user's account remains locked. Possible value is 1 to 480.
Account Inactivity	
Customize account inactivity threshold (days)	Specify the inactivity threshold that triggers disabling of inactive accounts. Possible value is 30 to 180.

Local Password Requirements

The **Local Password Requirements** page allows an administrator to change but not disable password security requirements by specifying password age, length, and complexity.

Field	Description
Password Management	
Maximum password age (days)	Specify at what age a password expires. Possible value is 30 to 180.
Minimum password age (days)	Specify how frequently a password can be changed. Possible value is 1 to 30.
Password warning interval (days)	Specify when users start to see a warning about their password expiration. Possible value is 1 to 7.
Minimum length	Specify the number of characters a password must contain. Possible value is 8 to 18.
Minimum changed characters	Specify the number of characters that must be different from the previous password. Possible value is 1 to 4.
Reject previous passwords	Specify how many of the user's previous passwords the system remembers and won't permit to be reused. Possible value is 8 to 16.

Field	Description
Password Complexity	
Lowercase letters	Specify the number of lowercase letters (a-z) that a password must contain. Possible value is 1 or 2.
Uppercase letters	Specify the number of uppercase letters (A-Z) that a password must contain. Possible value is 1 or 2.
Numbers	Specify the number of digit characters (0-9) that a password must contain. Possible value is 1 or 2.
Special characters	Specify the number of non-alphanumeric keyboard characters that a password must contain. Possible value is 1 or 2.
Maximum consecutive repeated characters	Specify how many sequential characters may be the same. Possible value is 1 to 4.

Reset System Passwords

The CMA system has several underlying service passwords. The **Reset System Passwords** page allows an administrator to reset these underlying service passwords. When you select this option, all of these underlying service passwords will be changed to the same obscured system-generated value.

Dial Plan and Sites

The **Dial Plan and Sites** workflow on a CMA system operating in maximum security mode has changed. The **Least Cost Routing** and **Services** menu options and their associated functionality are not displayed. Also, because the CMA system is not the gatekeeper, the CMA system **Site Topology** display is less informative. It used data provided to it by the gatekeeper functionality.

Backup System Settings

A CMA system operating in maximum security mode offers the **Backup System Settings** feature, which allows an administrator to create an archive that includes not only a backup of the CMA system databases but also all CMA system configuration settings.

The process for backing up the CMA system settings is documented in [“Backup Internal Databases and System Configuration”](#) on page 525.

To restore a system from a backup archive

- 1 **Restore the system to its factory default configuration.** You will need the **Restore to Factory Default DVD** that shipped with the CMA system server. This DVD has the base image of the CMA system server software.



WARNING

- This is a last resort, so never do this without being instructed to do so by PGS support.
- This process will wipe out your system database and all other system data.
- The **Restore to Factory Default DVD** is specific to the CMA system server type and version.

- 2 **Perform First Time Setup.** For more information about First Time Setup, see the *Polycom CMA System Getting Started Guide* for this release.
- 3 **Restore the system configuration** using the last archived configuration. The archived configuration will overwrite the configuration that resulted from First Time Setup. The only CMA system configuration settings not included in the archive and thus not overwritten are the network settings and the security certificates required for an operational system.

In cases when the CMA system is functional, but the configuration or database is corrupted, the backup archive can also be used to return a CMA system back to its last known good archive. As long as the network settings and security certificates are operational, the last known good archive will return the CMA system to its former functional state.

Network Intrusion Detection in Maximum Security Mode

The CMA system detects network intrusions by processing the Microsoft Windows Firewall logs, inserting dropped packet information into a temporary system database table, and identifying certain patterns in the data.

The CMA system detects the following types of intrusions: a fast port scan, a slow port scan, a denial of service (DoS) attack, and a flood attack. These are currently defined as:

- Fast port scan:
10 connections in a 5-second time period from the same source IP.
- Slow port scan:
100 connections in a 1-hour time period from the same source IP.
- DoS attack:
100 connections in a 5-second time period to the same destination port.
- Flood attack:
100 connections in a 5-minute window to any destination port from any source IP.

If the CMA system detects an intrusion, it displays a system alert on the user interface. The alert text will indicate the type of intrusion detected, such as:

- Port scan detected. See audit log for details.
- DoS attack detected. See audit log for details.
- Flood attack detected. See audit log for details.

Troubleshooting in Maximum Security Mode

Troubleshooting Utilities

A CMA system operating in maximum security mode has most of the same troubleshooting utilities of the standard commercial CMA system; however the **Traces** functionality has changed and functionality has been added. The following sections describe the troubleshooting utilities.

Windows Event Logs

There is no change in the **Windows Event Logs** function.

CMA System Logs

There is no change in the **CMA System Logs** function.

Database Backup

There is no change in the **Database Backup** function.

Test Network Connect

The **Test Network Connect** function allows you to perform a **Traceroute** or **Ping** operation. **Traceroute** allows you to investigate the route path and transit times of packets as they travel across an IP network. **Ping** allows you to test the availability of a host on an IP network.

Synchronize Certificate Stores

The **Synchronize Certificate Stores** function allows you to reset all certificate stores with the currently uploaded certificates and certificate revocation lists (CRLs).

Systems

The **Systems** pane displays summary information about the devices that access the CMA system. For a CMA system operating in maximum security mode, systems are limited to **Endpoints**, **MCUs**, and **Rooms**.

CMA Configuration

The **CMA Configuration** pane displays information about the configuration of the CMA system. For a CMA system operating in maximum security mode, configuration items are limited to **Software Version**, **Hardware Version**, **Enterprise Directory**, **Database**, **Time Source**, and **Enterprise Directory DC** (Domain Controller).

CMA Info

The **CMA Info** pane displays general information about the CMA system. For a CMA system operating in maximum security mode, this includes the following:

- Standard information:
CPU Utilization, Paging File Utilization, Last Hard Start/Reboot, Provisioning Operations in Progress operations, Software Update Operations in Progress, Hardware Alarms, Threshold Alarms, Temperature, Power Supply Status, Battery Status, and Cooling Fan Status.
- Additional information:
Total Memory, Free Memory, and Partition States.

CMA Licenses

There is no change in the **CMA Licenses** function.

Users Logged-In

The **Users Logged In** pane displays the type and number of users that are currently logged into the system. For a CMA system operating in maximum security mode, this includes a user role of **Auditor**.

Services

The **Services** pane displays information about the CMA system services, including the running services and the stopped services. For a CMA system operating in maximum security mode, there are 8 services rather than the 14 services in a commercial CMA system. The following table lists the services, their purpose, and whether or not they are essential to the health of a CMA system operating in maximum security mode.

Service	Manages the system's...	Comment
Apache2	Web processes	Essential
MSSQLSERVER	Database processes	Essential
OpenDS	Site topology database	Essential
openfire	Presence/XMPP processes	Not available
Polycom Cascader	Cascaded conferencing processes	Required for cascading conferences

Service	Manages the system's...	Comment
Polycom Conference Scheduling Service	Conference scheduling processes	Essential
Polycom Device Manager	Device management processes	Not Available
Polycom DialRuleService	Dial rule management processes	Essential
Polycom Gatekeeper	Gatekeeper processes	Not Available
Polycom JServer	Java processes including LDAP, SNMP, device management, Site Topology, and dynamically-managed device logins and provisioning.	Essential
Polycom Master Service	Basic operation processes	Essential
Polycom Serial COM	Serial port management processes	Not Available
Polycom Service Monitor	Redundancy monitoring processes	Not Available
Polycom Global Address Book	Global Address Book management processes	Not Available

Report Administration

The only **Report Administration** function supported on a CMA system operating in maximum security mode is the **Days to keep Conference and Endpoint CDRs**. All other **Report Administration** functions including creating and storing a weekly archive of the CDRs are not available.

Polycom® CMA® System Conference Scheduling Overview

This chapter provides an introduction to the Polycom® Converged Management Application™ (CMA®) system video conference scheduling functionality and operation. It includes these topics:

- [Conference Menu Overview](#)
- [General Scheduling Information](#)

To log into the CMA system web interface, you need:

- Microsoft Internet Explorer® 6.0, 7.0 or 8.0, Mozilla FireFox® 3.5 or 3.6, or Apple Safari 3.2, 4.0 or 5.0.

If your system is operating in maximum security mode, you may use only Microsoft Internet Explorer.

- Adobe® Flash® Player 9.x or 10.x
- The IP address or host name of the CMA system server and your username, password, and domain.



Note

The CMA system user interface is best viewed with an SXGA display resolution of at least 1280x1024 pixels. The minimum support display resolution is XGA 1024x768 pixels.

Generally, you get three opportunities to enter the correct password. After three failed attempts, the system returns an error message.

To log into a CMA system

- 1 Open a browser window and in the **Address** field enter the CMA system IP address or host name.
 - If prompted to install the Adobe Flash Player, click **OK**.
 - If you receive an **HTTPS Security Alert**, click **Yes**.

- If you see a login banner, click **Accept** to accept the terms and continue.

If you cannot connect to the system, there may be certificate issues.

- 2 When the CMA system **Log In** screen appears, enter your **Username** and **Password**.
- 3 If necessary, select a different **Language** or **Domain**.
- 4 Click **Login**.

If you log in as an administrator, you see the CMA system **Dashboard**.

For more information about roles and the functionality associated with roles, see [“Default CMA System Roles and Permissions”](#) on page 253.

Conference Menu Overview

This section includes some general information you should know about the Conference menu and views. It includes these topics:

- [Conference Menu and Views](#)
- [Conference Views—Future and Ongoing](#)
- [Conference States](#)
- [Context-Sensitive Conference Actions](#)



Conference Menu and Views

The **Conference** menu provides these views of the **Conference** list:

- **Future**—Displays the list of future conferences in the main window. Use this view to view and edit future conferences.
- **Ongoing**—Displays the list of active conferences in the main window. Use this view to manage ongoing conferences.




Users can only work with the conferences that appear in their **Conference** list. By default, schedulers see only their conferences in the **Conference** list, while operators see all the conferences on the system. However, when areas are defined, operators see all the conferences for the areas to which they belong. By default, users assigned other roles cannot view conferences.


The **Conference** views have these sections.

Section	Description
Views	The views you can access from the page.
Conference Actions	<p>The set of available commands. The constant commands in the Conference views are:</p> <ul style="list-style-type: none"> • Refresh  —Use this command to update the display with current information. • Add  —Use this command to create a new video and/or audio conference.
Conference List	The context-sensitive Conference list for the selected view.
Conference Details	Displays information about the selected conference. For more information, see “Conference Details” on page 81.
Conference Features	Displays the status of system features for the selected conference. For more information, see “Conference Features” on page 83.
Bridge (MCU) Features	Displays the status of MCU features for the selected conference. For more information, see “Bridge (MCU) Features” on page 84.
Participants	Displays the list of participants for the selected conference. For more information, see “Participants List” on page 85.
Participant Details	Displays information about the participant selected in the Participants list. For more information, see “Participant Details” on page 86.

Conference Views—Future and Ongoing





The **Conference** list in both the **Future** and **Ongoing** view has these fields.



Field	Description
Filter	<p>Use the filter to display other views of the conference list, which include:</p> <ul style="list-style-type: none"> • Future Only - Displays scheduled conferences that have not yet started • Today Only - Displays scheduled conferences (completed, active, or future) for the current day and active ad hoc conferences • Custom Date - Displays scheduled conferences (completed, active, or future) for a selected day. Select the day from the calendar. • Ongoing Plus - Displays active and future scheduled conferences for the day. You can further filter this request by Owner, Conference Name, Endpoint Name, and Bridge. • Today Plus - Displays scheduled conferences (completed, active, or future) for the current day, current ad hoc conferences, and all future conferences. You can further filter this request by Owner, Conference Name, Endpoint Name, and Bridge. • Yesterday Plus - Displays completed scheduled conferences for yesterday and earlier. You can further filter this request by Owner and Conference Name. <p>These filters apply to scheduled conferences only. Ad hoc conferences are not displayed in the filtered list.</p> <p>For information on filters, see “Filter and Search a List”.</p>
Export as Excel file	Click this button to download the currently displayed Conference list to a Microsoft Excel spreadsheet.
Status	The state of the conference. For more information, see “Conference States” on page 43.
Type	<p>The type of scheduled conference. Possible values include:</p> <ul style="list-style-type: none"> • Video Conference  —All conference participants have video endpoints. • Audio Only Conference  —All conference participants have audio endpoints. Audio only conferences require an MCU. • Recurring Conference  —The conference is one in a recurring series. • Multi-Bridge Conference —The scheduler assigned the conference to multiple bridges and created bridge links.

Field	Description
Conference Name	The system- or scheduler-assigned name of the conference. By default, the system assigns a conference name and appends the day and date to that name. The scheduler can change the system-assigned name.
Start Time	The user-assigned start time for the conference. The system appends the time difference between the local time and the standard time.
Bridge	If applicable, the user-assigned bridge for the conference. Possible values are: <ul style="list-style-type: none"> N/A—A bridge is not required for the conference. <Bridge Name>—The user assigned the conference to a single bridge. In this case, the bridge name is displayed. Multi bridge —The user assigned the conference to multiple bridges and created bridge links.
Owner	The conference creator.

Conference States






Conferences may be in the following states.

State	Description
Future Conference 	Scheduled conference that has not yet started. This conference state is possible in all views except the Yesterday Plus view.
Completed Conference 	A scheduled conference that occurred in the past. This conference state is possible in all views except the Future and Ongoing Plus view.
Active Conference 	A conference that is still active/ongoing. This conference state is possible in all views except the Future and Yesterday Plus view.
Active Alerts Conference 	The bridge on which the active/ongoing conference is being hosted has sent an alert. Examples of events that will trigger a bridge alert are: <ul style="list-style-type: none"> A participant is connected in secondary mode (audio only). A conference is not yet full (i.e., not all scheduled participants have joined the conference).

State	Description
Declined Conference 	Applies only to conferences scheduled through the Polycom Scheduling Plugin for Microsoft Outlook. This state indicates that most participants did not accept the conference invitation. If your system is in maximum security mode, the Polycom Scheduling Plugin for Microsoft Outlook is not available.
Conference End Warning 	The conference is ending, i.e., it is in its last five minutes unless someone extends it.

Context-Sensitive Conference Actions

Besides the constant **Refresh**  and **Add**  actions, the **Conference Actions** section may include these context-sensitive actions depending on the type of conference selected.

Action	Description
Available for future conferences only	
Edit 	Use this command to edit the selected conference. For more information, see “Edit a Conference” on page 56.
Available for future and past conferences	
Delete 	Use this command to delete the selected conference.
Available for future, past, and active conferences	
Copy 	Use this command to copy the selected conference.
Available for active conferences only	
Manage 	Operators only. Use this command to display the Manage Conference page for the conference selected in the Conference List . Use this command to manage participants and endpoints in the selected active conference. For more information, see “Manage an Active Conference” on page 69.
Terminate 	Operators only. Ends the selected conference.

General Scheduling Information

You may find the following general topics useful when you are scheduling conferences.

- [Scheduling Participants and Endpoints](#)
- [Bridge Selection and Cascading](#)
- [Bridge Scheduling and Reassignment](#)

Scheduling Participants and Endpoints

When you schedule conferences, you select the participants you wish to join the conference from your endpoint directory. Depending on your system configuration, your endpoint directory may be the enterprise directory, the Global Address Book, or one or more local address books. It may also include Guest Book entries.

For participants that have multiple endpoints registered with the CMA system, the system selects the participant's default endpoint. You can change to another endpoint by selecting it from the **Call Info** list or by editing the participant.

You can schedule participants without endpoints into conferences. You cannot schedule endpoints without owners into conferences. The CMA system can be configured to allow you to overbook dial-in participants. In this case, dial-in participants can be scheduled to dial into multiple conferences during the same time period, but the system reserves resources for the participant for only the first scheduled conference. Dial-out participants cannot be scheduled into multiple conferences.

Also, if you schedule participants into conference as **Dial In** participants, the conference will require external MCU resources.

Bridge Selection and Cascading

When a conference is scheduled with one of the CMA system scheduling applications (Web Scheduler or Scheduling Plug-in for Microsoft Outlook or IBM Lotus Notes) and the conference requires external MCU resources (such as a Polycom RMX or MGC system), then by default the CMA system automatically assigns the conference to a bridge. However, the system allows users with the **Advanced Scheduler** role to select a bridge for their conferences. It also allows them to create multibrige, cascaded conferences.

Bridge Selection

When scheduling a conference, users with the **Advanced Scheduler** role can select a bridge to host their conference by selecting the **Single Bridge** option. When they select this option, the system presents a list of bridges that have the capabilities and resources required to host their conference.

Because this bridge list depends on the template selection, users should make their template selection before selecting a bridge. Otherwise, they may select a bridge that cannot meet their conferencing requirements. In this case, the conference will fail to schedule.

Bridge Selection and Cascading Conferences

When scheduling a conference, users with the **Advanced Scheduler** role can select the **Multi Bridge** option to create cascading conferences.

In some respects, a cascaded conference looks like a single conference, but it is actually two or more conferences on different bridges that are linked together. The link is created by a dial-out from one conference to a second conference via a special cascaded entry queue.

Some reasons you may wish to create cascading conferences include:

- To invite more conference participants than any single bridge can host
- To connect different bridges at different sites into a single conference
- To use the different capabilities of different bridges (for example, different communication protocols, such as, serial connections, ISDN, etc.)

When you create a multibridge, cascaded conference, you must manually select bridges and create the cascaded links between bridges by identifying the originating bridge, the terminating bridge, and the network type (IP or ISDN). The system displays an interconnection diagram that illustrates the cascaded links. Once scheduled, each cascaded link appears as a participant in the conference.

By default, the system automatically assigns participants to the “best bridge” for them based on available capacity, location, and least cost routing rules. However, you may also choose to manually assign participants to bridges.

Bridge Scheduling and Reassignment

When a conference is scheduled with one of the CMA system scheduling applications (Web Scheduler or Scheduling Plug-in for Microsoft Outlook or IBM Lotus Notes), by default the system automatically assigns the conference to a bridge unless a user with the default **Advanced Scheduler** role intercedes. If that bridge is down at the time the system starts the conference, the CMA system attempts to dynamically reassign the conference to another bridge with sufficient capabilities and resources.

- If the system can successfully reassign the conference to another bridge, the conference starts on the newly selected bridge, and the system sends an updated conference email to all scheduled participants. This updated email includes a new dial-in number that dial-in participants must use to join the conference.
- If the system cannot successfully reassign the conference to another bridge, the conference fails to start. The system sends an email to notify the conference organizer of the failure.

Some notes about bridge reassignment:

- The bridge reassignment process only occurs when the system detects that a bridge is down. It does not occur if the system determines that a bridge does not have sufficient resources required to host the conference.
- If the CMA system cannot find another bridge with the features and capacity needed to support a conference, the conference fails to start. The system does not attempt to modify the conference settings in any way. Instead, the system sends an email to notify the conference organizer of the failure.
- The system will chain bridge reassignments. This means that if the next bridge to which the system assigns a conference is down at the time the system tries to start the conference, the system will try to reassign the conference again.
- If the bridge to which the system reassigns a conference has ad hoc conferences on it, the CMA system is unaware of those conferences. The reassigned conference may fail to start if ad hoc conferences are consuming resources the CMA system expected to schedule. This is known behavior and is avoided by applying the best practice of not using bridges for both scheduled and ad hoc conferences.

Conference Scheduling Operations

This chapter describes the Polycom® Converged Management Application™ (CMA®) system conference scheduling operations. It includes these topics:

- [Add/Schedule a Conference](#)
 - [Add/Schedule a New Conference](#)
 - [Copy an Existing Conference](#)
- [Edit a Conference](#)
- [Edit a Participant's Settings](#)
- [View Scheduling Information for a Conference](#)

Add/Schedule a Conference

By default, only schedulers and operators can schedule conferences.


Schedulers have two options for scheduling a new conference:

- [Add/Schedule a New Conference](#)
- [Copy an Existing Conference](#)

These options are discussed in the following topics.

Add/Schedule a New Conference

To add or schedule a new conference

- 1 Go to **Conference > Future** and click **Add** .
- 2 In the conference scheduling page, enter a **Conference Name** and set a conference **Start Date**, **Start Time**, and either an **End Time** or **Duration**.

- 3 To make the conference recurring, click **Recurrence** and in the **Appointment Recurrence** dialog box, set:
 - Recurrence frequency (**Daily**, **Weekly**, or **Monthly**)
 - Recurrence day (Sunday through Saturday)
 - Recurrence range (**Start** date and **End After** occurrences or **End by** date)

The maximum number of recurrences is 365.

 - Click **OK**.
- 4 For an **Audio Only** conference, change the **Conference Type** to **Audio Only**.
- 5 To change the template, click **Default Template** or **Default Audio Template** and select a different template, if available.



Notes

- Conference templates provide default conference settings. When you select a different template, you are selecting the default conference settings for your conference.
- The **Default Template** and **Default Audio Template** are available to all users who can schedule conferences. Other templates may also be available if they have been assigned to users with your role.
- The **Default Template** and **Default Audio Template** are stored in the system database and their names are not localized.

- 6 To add conference participants from the local directory or enterprise directory:
 - a Enter all or part of a participant's **Last Name** or **First Name** into one of the name fields and click **Add Participants**.

The **Add Participants** dialog box appears with the list of participant names that meet your search criteria.



Notes

- Depending on the search domain, the search function may return different results. See ["Filter and Search a List"](#) on page 4.
- The search results only include participants associated with endpoints.

- b Select the participant of interest's name from the list.

The participant's name appears in the underlying **Selected Participants and Rooms** list.
- c Repeat steps a and b to add all domain participants and then click **Close**.

- 7 To add a guest from the **Guest Book**:
 - a Click **Add From Guest Book**.
 - b In the **Add From Guest Book** dialog box, select the guest of interest's name from the list.

The guest's name appears in the underlying **Selected Participants and Rooms** list.
 - c Repeat step b to add all participants from the **Guest Book** and then click **Close**.
- 8 To add new guest participants (participants not available through the local directory, enterprise directory, or **Guest Book**):
 - a Click **Add Guest**.
 - b Configure these fields in the **Add Guest** dialog box.

Field	Description
First Name	The guest's first name.
Last Name	The guest's last name. Note The system allows you to add multiple users with the same first and last name into the Guest Book .
Email	The guest's E-mail address. The system only validates the structure of the E-mail address. Note The E-mail field is ASCII only.
Location	The location of the guest's endpoint system. This is a free-form field that the system does not validate.
How will the participant join the conference	Specify how the participant will join the conference. <ul style="list-style-type: none"> • In Person —The participant will attend the conference by going to a room that is included in the conference or joining another participant who is attending the conference. • Audio Only —The participant will attend the conference by telephone. The system will either call out to the participant or the participant will dial in. • Use Video—The participant will attend the conference using a video endpoint system. The system will either call out to the participant or the participant will dial in. This selection will in part determine what other fields of the Add Guest dialog box you will need to complete.

Field	Description
Bit Rate	(Video only) Set as required. You can change the connection speed for an endpoint up to the maximum speed specified by the conference template.
Dial Options	Specify whether the guest will dial into the conference or require that the system dial out to the guest.
Dial Type	Specify the protocol that the guest's endpoint supports: H.323 (IP), SIP (IP), or H.320 (ISDN). This selection will determine what other sections of the Add New Guest dialog box you will need to complete.

- c If the guest has an **H.323 (IP)** endpoint, configure these settings:

Field	Description
Number and Number Type	<p>The specific dial string for the guest, and the format of the number that the MCU must resolve to contact the guest. This may be an IP address, E.164 address, H.323, or Annex-O.</p> <p>For Annex-O dialing, in the Number field enter the <i>H.323.alias@IP</i>, for example:</p> <ul style="list-style-type: none"> • <i>1001@11.12.13.14</i> • <i>1001@domain.com</i> • <i>username@domain.com</i> • <i>username@11.12.13.14</i> <p>Notes</p> <ul style="list-style-type: none"> • Polycom endpoints must register with a gatekeeper before they will attempt an Annex-O call. • You can enter a dial string for another MCU as a guest. If so, you may need to specify the conference ID in the Extension field also.
Extension	Use this field to connect the conference to another conference on another MCU. In this field, specify the conference ID or passcode for the conference on the other MCU.
MCU Service	Choose from the list of MCU services defined on the MCUs with which the CMA system is registered. Leave this at Any Available Service unless you have specific knowledge of MCU services.

- d** If the guest has a **SIP (IP)** endpoint, configure these settings:

Field	Description
Sip URI	The SPI URI the MCU must resolve to contact the guest.
MCU Service	Choose from the list of MCU services defined on the MCUs with which the CMA system is registered. Leave this at Any Available Service unless you have specific knowledge of MCU services.

- e** If the guest has an **H.320 (ISDN)** endpoint, configure these settings:

Field	Description
Use Modified Dial Number	Select this option first (as needed) as it will determine the other fields you must configure.
Country	(Not available when Use Modified Dial Number is selected.) The country to which the system will dial out to the guest. Click Select to view a list of country codes.
Area/City Code	(Not available when Use Modified Dial Number is selected.) The area code to which the system will dial out to the guest.
Number	The participant's phone number.
Extension	Cannot be configured.
MCU Service	Choose from the list of MCU services defined on the MCUs with which the CMA system has registered. Leave this at Any Available Service unless you have specific knowledge of MCU services.

- f** Select **Save to Guest Book** to have this guest participant added to the system **Guest Book**.

- g** Click **OK**.

The guest's name appears in the **Selected Participants and Rooms** list.

- 9** Adjust the conference date and time as needed to match participant and endpoint availability.

- a Review their availability and adjust the conference date and time as needed.



Notes

- For participants who are associated with endpoints, the CMA system schedules their availability according to the endpoint's availability.
- For participants with multiple endpoints, check the availability for each endpoint. Click **Call Info** to change the participant's endpoint.
- Dial-in participants can be scheduled to dial into multiple conferences during the same time period; dial-out participants cannot.

- b To edit a participant's dial settings, select the participant from the **Selected Participants and Rooms** list and click **Edit**. For more information on editing participants settings, see "[Edit a Participant's Settings](#)" on page 57.

10 To add conference rooms to the **Selected Participants and Rooms** list:

- a Click **Select Site**.
- b Select the site of interest from the site list.
The conference room list for the selected site appears.
- c Select the conference room of interest from the list.
The conference room name appears in the underlying **Selected Participants and Rooms** list.
- d Repeat steps b and c to add all required conference rooms and then click **OK**.

11 If you have the **Advanced Scheduler** role, now is the time to assign conference leadership roles, edit conference settings, and make bridge selections. For more information, see "[Advanced Scheduling Operations](#)" on page 61.

12 To edit a participant's dial settings, select the participant from the **Selected Participants and Rooms** list and click **Edit**. For more information on editing participants settings, see step 5 on page 57.

13 When finished, click **Schedule**.

The system verifies that it has a bridge with the capabilities and resources required for your conference. If it does, the conference notification E-mail appears with a message indicating **Conference Successfully Scheduled**.

14 To exit without sending an E-mail to participants, click **Skip Email**.

15 To send an E-mail notification to participants:

- a Copy additional people on the notification and/or add notes about the conference.

Note that the **To**, **CC**, and **BCC** fields are ASCII only.

- b** As needed, add information in the **Enter additional notes to include in the email** section.
- c** Click **Send**.

The system sends the conference notification E-mail. The **Future** view appears. The conference appears in the conference list.


The E-mail that the CMA system sends can be read by E-mail systems that accept plain text E-mails, iCal attachments, or vCal attachments.

Copy an Existing Conference

Future, ongoing, or past conferences can be copied as a template for a future conference.

Users can only copy conferences that appear in their **Conference** list. By default, schedulers see only their conferences in the **Conference** list, while operators see all the conferences on the system, unless areas are defined. In which case operators see all the conferences for the areas to which they belong. By default, users assigned other roles cannot view conferences.

To copy a conference

- 1** Go to the appropriate conference view.
- 2** Select the conference of interest and click **Copy** .
- 3** If you used a template other than the default when you created the conference, reselect the template.
- 4** Make the required changes to the conference date, participants, rooms, or other settings. For information on performing these tasks, see [“Add/Schedule a Conference”](#) on page 49.
- 5** When finished, click **Schedule**.

The system verifies that it has a bridge with the capabilities and resources required for your conference. If it does, the conference notification E-mail appears with a message indicating **Conference Successfully Scheduled**.


- 6** To exit without sending an updated E-mail to your participants, click **Skip Email**.

Edit a Conference

Only future conferences can be edited. Active or past conferences cannot be edited.

Users can only edit the conferences that appear in their **Conference** list. By default, schedulers see only their conferences in the **Conference** list, while operators see all the conferences on the system, unless areas are defined. In which case operators see all the conferences for the areas to which they belong. By default, users assigned other roles cannot view conferences.

To edit a future conference

- 1 Go to **Conference > Future**.
- 2 Select the conference of interest and click **Edit** .
- 3 If you select a recurring conference, a dialog box appears asking if you want to edit all conferences in the series or just the selected one. Make the appropriate choice and click **Edit**.

The conference scheduling page appears.

- 4 To change the template, click **Default Template** or **Default Audio Template** and select a different template, if available.



Notes

- Conference templates provide default conference settings. When you select a different template, you are selecting the default conference settings for your conference.
- The **Default Template** and **Default Audio Template** are available to all users who can schedule conferences. Other templates may also be available to you if they have been assigned to users with your role.
- The **Default Template** and **Default Audio Template** are stored in the system database and their names are not localized.

- 5 Make the required changes to the conference date, participants, rooms, or other settings. For information on performing these tasks, see [“Add/Schedule a Conference”](#) on page 49.
- 6 When finished, click **Schedule**.
The system verifies that it has a bridge with the capabilities and resources required for your conference. If it does, the conference notification E-mail appears with a message indicating **Conference Successfully Scheduled**.
- 7 To exit without sending an updated E-mail to your participants, click **Skip Email**.


- 8** To send an updated E-mail to your participants:
 - a** Copy additional people on the notification and/or add notes about the conference.
Note that the **To**, **CC**, and **BCC** fields are ASCII only.
 - b** Click **Send**.
The system sends the updated conference notification E-mail. The **Future** view appears. Your conference appears in the conference list.

Edit a Participant's Settings

Participant's settings for future scheduled conferences may be edited. Schedulers cannot edit a participant's settings for an active or past conference.

Users can only work with the conferences that appear in their **Conference** list. By default, schedulers see only their conferences in the **Conference** list, while operators see all the conferences on the system, unless areas are defined. In which case operators see all the conferences for the areas to which they belong. By default, users assigned other roles cannot view conferences.

To edit a participant's settings

- 1** Go to **Conference > Future**.
- 2** Select the conference of interest and click **Edit** .
- 3** If you select a recurring conference, a dialog box appears asking if you want to edit all conferences in the series or just the selected one. Make the appropriate choice and click **Edit**.
- 4** In the conference scheduling page, select the participant of interest from the **Selected Participants and Rooms** list and click **Edit**.
- 5** In the **Edit Participant Settings** dialog box, edit the participant settings as required.

- a** If the guest has an **H.323 (IP)** endpoint, configure these settings:

Field	Description
Number and Number Type	<p>The specific dial string for the guest, and the format of the number that the MCU must resolve to contact the guest. This may be an IP address, E.164 address, H.323, or Annex-O.</p> <p>For Annex-O dialing, in the Number field enter the <i>H.323.alias@IP</i>, for example:</p> <ul style="list-style-type: none"> • <i>1001@11.12.13.14</i> • <i>1001@domain.com</i> • <i>username@domain.com</i> • <i>username@11.12.13.14</i> <p>Notes</p> <ul style="list-style-type: none"> • Polycom endpoints must register with a gatekeeper before they will attempt an Annex-O call. • You can enter a dial string for another MCU as a guest. If so, you may need to specify the conference ID in the Extension field also.
Extension	Use this field to connect the conference to another conference on another MCU. In this field, specify the conference ID or passcode for the conference on the other MCU.
MCU Service	Choose from the list of MCU services defined on the MCUs with which the CMA system is registered. Leave this at Any Available Service unless you have specific knowledge of MCU services.

- b** If the guest has a **SIP (IP)** endpoint, configure these settings:

Field	Description
Sip URI	The SPI URI the MCU must resolve to contact the guest.
MCU Service	Choose from the list of MCU services defined on the MCUs with which the CMA system is registered. Leave this at Any Available Service unless you have specific knowledge of MCU services.

- c If the guest has an **H.320 (ISDN)** endpoint, configure these settings:

Field	Description
Use Modified Dial Number	Select this option first (as needed) as it will determine the other fields you must configure.
Country	(Not available when Use Modified Dial Number is selected.) The country to which the system will dial out to the guest. Click Select to view a list of country codes.
Area/City Code	(Not available when Use Modified Dial Number is selected.) The area code to which the system will dial out to the guest.
Number	The participant's phone number.
Extension	Cannot be configured.
MCU Service	Choose from the list of MCU services defined on the MCUs with which the CMA system has registered. Leave this at Any Available Service unless you have specific knowledge of MCU services.

- 6 Click **OK**.

View Scheduling Information for a Conference

Users can only view scheduling information for the conferences that appear in their **Conference** list. By default, schedulers see only their conferences in the **Conference** list, while operators see all the conferences on the system, unless areas are defined. In which case operators see all the conferences for the areas to which they belong. By default, users assigned other roles cannot view conferences.

To view the scheduling information for a conference

- 1 To see the scheduling information for a future conference, go to **Conference > Future**. To see the scheduling information for an active conference, go to **Conference > Ongoing**.
- 2 From the list of **All Conferences**, select the conference of interest and click **View**.

The **View** conference page appears displaying the following details about the conference:

Section	Description
Start Date	The date on which the conference started or will start.
End Date	The date on which the conference is scheduled to end.
Duration	The scheduled duration of the conference in hours and minutes.
Recurrence	The recurrence information for the conference.
Owner	The person who scheduled the conference.
Type	The type of conference as identified by an icon. Hover over the icon to determine the conference type.
Conference Passcode	The conference passcode assigned to the conference. For future conferences, users with the Advanced Scheduler role can change this conference password. See “Edit Conference Settings” on page 61.
Chairperson	Whether or not the conference has a chairperson. This field will include a participant’s name or N/A. For future conferences, users with the Advanced Scheduler role can assign a conference chairperson. See “Edit Conference Settings” on page 61.
Participants List	Information for the participant, including <ul style="list-style-type: none">• Name• Dial Mode• Participant Type• Access• Endpoint

- 3 Click **Back to List** to return to the conference list.

Advanced Scheduling Operations

This chapter describes how users with the **Advanced Scheduler** role have more options when scheduling conferences using the Polycom® Converged Management Application™ (CMA®) system.

When scheduling conferences, advanced schedulers can:

- [Edit Conference Settings](#)
- [Select a Bridge for a Conference](#)
- [Create a Cascaded Conference Across Multiple Bridges](#)

Edit Conference Settings

By default, users with the **Advanced Scheduler** role can overwrite certain conference template settings as described here.



Note

Two conferences scheduled with the same template may have different settings and behavior if they are hosted on different types of MCUs. Minimize or eliminate such differences by ensuring that all MCUs are similarly configured and that all CMA system templates are synchronized with RMX profiles.


Schedulers can edit conference settings only for scheduled conferences. They cannot edit conference settings for active conferences.

To edit the conference settings

- 1 On the conference scheduling page, as you are adding or editing a conference, click **Edit Conference Settings**.

- 2 As needed, configure these settings on the **Conference Settings** dialog box. The settings that you can edit may depend on the template selected.

Setting	Description
Conference ID	<p>By default, the system assigns a Conference ID. You can change this ID to permit integration with third-party scheduling tools. This identifier must be 8 or less numeric digits.</p> <p>Notes</p> <ul style="list-style-type: none"> The CMA system compares the Conference ID to its database to verify that it is unique. If it is not unique, you will be prompted to enter a new Conference ID. If a conference is scheduled on a Polycom RMX system and the room ID is the same as the assigned Conference ID, then the conference will not be created on RMX. The conference will launch on the CMA system with an active status, but will display no endpoints connected.
Conference Passcode	<p>By default, the system assigns an 15-digit Conference Passcode and provides this passcode to participants within the content of the conference notification E-mail. You can change this passcode to another 9- through 16-digit number.</p>
Enable Chairperson	<p>You can select a video chairperson to control the conference from his or her video endpoint system. The video chairperson must have a video endpoint system and Chairperson conferences require an MCU.</p> <p>Notes</p> <ul style="list-style-type: none"> If the conference template has the Conference Requires Chairperson parameter enabled, then Enable Chairperson is automatically selected and cannot be changed. If a conference is scheduled on a Polycom RMX system and the RMX profile has Conference Requires Chairperson selected but the template does not, and the conference is scheduled without a chairperson, then all users will remain in the waiting room and will not be able to join the conference. Polycom RMX 1000 systems do not support the Chairperson feature.

Setting	Description
Chairperson Passcode	<p>If Enable Chairperson is selected, the system assigns an 15-digit Chairperson Password and provides this password to the video chairperson in a separate E-mail.</p> <p>If Enable Chairperson is selected, the chairperson must enter this 15-digit password at his or her video endpoint to assume control of the conference.</p> <p>You can change this password to another 4- through 16-digit number.</p>
Dial Options	<p>You have three options:</p> <ul style="list-style-type: none"> To create a conference for which the same dial-in information and a PIN code are assigned to all conference participants, use the Dial-In setting. This setting allows participants to dial in from an audio or video endpoint and connect to the same conference on the MCU. To dial out to all participants in the conference, use the Dial-Out setting. To allow participants both options, select Dial-In+Dial-Out. <p>Note</p> <p>When you change a conference from Dial-In to Dial In+Dial Out, the selected resources remain set to Dial-In. You must change them manually.</p>
Always Use MCU	<p>This setting forces the conference to an MCU and prevents video endpoints from connecting to each other directly. This setting is automatically selected and cannot be changed when Audio Only is the conference type or when Enable Chairperson is selected.</p>
Video Mode	<p>Determines the initial layout on a video endpoint's monitor for a multipoint conference that requires an MCU. The options are:</p> <ul style="list-style-type: none"> Switching.  Indicates that the display changes each time the speaker changes, and everyone sees the current speaker. Select a Frame Count, then select the specific layout for the frames. <p>The available layouts are Continuous Presence settings.</p>

Setting	Description
Bit Rate	<p>Specifies the maximum connection speed for endpoints in the conference. Individual endpoints that specify a lower connection speed connect at that lower speed. Endpoints that specify a higher connection speed connect at the speed identified in the conference template.</p> <p>If you select a higher speed than an endpoint can support, the system reduces the speed that endpoint; however, the conference uses the default connection speed for endpoints that can match it. If you place the calls through an endpoint with an embedded MCU, the behavior depends on the capabilities of that endpoint.</p>
Bit Rate (<i>continued</i>)	<p>When the dial speed is higher than the number of channels defined in the H.320 service for the endpoint, you receive a warning. To continue, lower the dial speed to less than or equal to the ISDN capability of the endpoint.</p> <p>Higher speed is important for high-quality video in a conference. Because higher speeds use greater bandwidth, scheduling a high-bandwidth conference may limit the number of conferences that you can reserve at one time.</p>

Setting	Description
People + Content	<p>Controls the ability for one endpoint to send two types of data—a data stream and a video stream—over the same bandwidth to display people and content. The receiving endpoint handles the two video streams differently and may display them on separate screens or through video switching mode.</p> <p>Endpoints that do not support the selected method connect with either video through IP or audio only through ISDN.</p> <p>Select from these available settings:</p> <ul style="list-style-type: none">• None. Select this option when dual data streams are not required.• People +Content (H.329). This enables the industry standard H.239 dual streams for endpoints that support H.239 or the Polycom proprietary People + Content dual streams for older Polycom endpoints without H.239 capabilities. The MCU requires that conferences with People + Content use a minimum speed of 192 K.• People and Content VO. This Polycom proprietary technology works with PictureTel endpoints. Select this option for older endpoints.• Visual Concert PC. Select this option for use with Polycom ViewStation MP/512/SP/323 endpoints.• Visual Concert FX. Select this option for use with Polycom ViewStation FX/EX and VS4000 endpoints.• Duo Video. This setting supports IP and ISDN and is available with TANDBERG endpoints, in which one part of the conference is set as the video conference and the other as the presentation conference.

Setting	Description
T.120 Mode	<p>For MGC-hosted conferences only, selects the protocols and specifications for multipoint data communication.</p> <p>If your system is in maximum security mode, the T.120 options are not supported.</p> <p>In the T.120 menu, select the speed for the T.120 connection. See your IT department to determine the best combinations for your conferences. To disable the T.120 mode, select None.</p> <p>If you select T.120, these options may be available, according to the participant's endpoint and software:</p> <ul style="list-style-type: none"> • Application Sharing. Allows two or more participants to work on the same document or application, even when only one participant has the application. In application sharing, one participant launches the application, and it runs simultaneously on all other computers. • File Transfer. Enables participants to send files to each other. • Chat or Whiteboard. Allows participants to communicate with each other by writing. <p>In all of these modes, participants can view and hear each other.</p>

- 3 If the conference is configured for **Chairperson** or **Lecturer** modes, assign participants leadership roles:
 - a To assign a participant the lecturer role, in the **Lecturer** field select the participant's name from the list.
 - b To assign a participant the video chairperson role, in the **Video Chairperson** field select the participant's name from the list.



Notes

- If the **Lecturer** or **Video Chairperson** features are not available, then the selected template does not support these features.
- To be assigned **Lecturer**, a participant must have a manageable video endpoint.

- 4 Continue on to [“Select a Bridge for a Conference”](#) on page 67, as required, or return to adding or editing the conference, as described in [“Conference Scheduling Operations”](#) on page 49.

Select a Bridge for a Conference

By default, when scheduling a conference, the CMA system will automatically select a bridge for the conference. However, users with the **Advanced Scheduler** role can select a specific bridge for a conference.

To select a single bridge for a conference

- 1 When you're adding or editing a conference, after you've made all of your other conference configuration choices, from the **Bridge Selection** list select **Single Bridge**.

A bridge selection drop down list appears based on the template selection and conference settings.

- 2 From the MCU list, select a specific MCU to host the conference.
- 3 Continue on to ["Create a Cascaded Conference Across Multiple Bridges"](#) on page 67, as required, or return to adding or editing the conference, as described in ["Conference Scheduling Operations"](#) on page 49.

Create a Cascaded Conference Across Multiple Bridges

Users with the **Advanced Scheduler** role can create cascaded conferences.

To create a cascaded conference across multiple bridges

- 1 When you're adding or editing a conference, after you've made all of your other conference configuration choices, from the **Bridge Selection** select **Multi Bridge**.



Note

If the **Multi Bridge** option is not available, then the system is not configured to support this option.

The **Schedule** button changes to a **Manual Cascade** button and the **Recurrence** button is grayed out.

- 2 Click **Manual Cascade**.

The **People To Bridges** dialog box appears displaying the selected conference participants and their bridge assignments. Bridge assignments default to **Auto**. These system assignments are based on bridge capacity and/or least cost routing principles.

In the **Selected Bridge Availability** section, the system shows a count of the available ports on the available bridges for the specified time period.

If the port count is within 5% of the maximum ports available, it is displayed in red.

- 3 To change a bridge assignment for a selected participant, click **Auto** and select a bridge from the pull-down menu.



Note

A CMA system can only show port counts for conferences scheduled via the system. Ad hoc conferences are not included in the port count.

- 4 When you've completed all bridge assignments, click **Next**.

The **Bridge To Bridge Links** dialog box displays a graphical view of the selected bridges.



Note

If an MCU does not show up in the **Bridge To Bridge Links** dialog box, then the MCU software does not support cascading.

- 5 To add a hub bridge (a bridge used to connect one bridge to another), from the **Available Bridges** window, select a bridge and click **Add Bridge**.
- 6 Specify bridge-to-bridge connections by selecting the bridges of interest and clicking **Add Link**.

The link is graphically represented by an arrow. The bridge at the base of the arrow dials to the bridge at the point of the arrow.



Note

A Polycom RMX system cannot dial a Polycom MGC, so do not link from an RMX system to an MGC system.

- 7 In the **Add Link** dialog box, select the **Link Type**.



Notes

- You can add links from a Polycom MGC system to a Polycom RMX system.
- There is no support for ISDN cascaded links on RMX MCUs.
- The lag time required to update cascaded links may cause more than one participant to hear the prompt about being the first person to join the conference.

- 8 Return to adding or editing the conference, as described in "[Conference Scheduling Operations](#)" on page 49.

Conference and Participant Management Operations


This chapter describes the Polycom® Converged Management Application™ (CMA®) system conference and participant management operations. It includes these topics:

- [Manage an Active Conference](#)
- [Add Additional Participants to an Active Conference](#)
- [Add a Room to an Active Conference](#)
- [View the Video of a Participant in an Active Conference](#)
- [Join an Active Conference](#)
- [Add a Participant from a Favorites List to an Active Conference](#)
- [Add/Save a Participant to a Favorites List](#)
- [Manage a Participant's Endpoint During a Conference](#)
- [View a Participant's Details During a Conference](#)
- [Terminate an Active Conference](#)
- [Delete a Conference](#)

Manage an Active Conference

The **Manage Conference** page provides a detailed view of a single active conference and allows an operator to make some changes to the conference.




To manage an active conference



- 1 Go to **Conference > Ongoing**.
- 2 From the list of **All Conferences**, select the conference of interest and click **Manage** .

The conference page appears in a new tab displaying the **Participants** list. The **Participants** list displays these settings:









Section	Description
Status	The state of the participant's connection as identified by an icon. Hover over the icon to determine the status.
Type	The type of conference as identified by an icon. Hover over the icon to determine the type.
Name	The participant's name.
Endpoint	The name assigned to the participant's endpoint when it registered or was added to the system.
Access	The endpoint's network interface type. Possible values include: <ul style="list-style-type: none"> H323 ISDN
Address	The IP address or ISDN number of the participant's endpoint (if a dial-out).
Bit Rate	The sum of the audio and video data transfer rate (in kbps) of the participant's endpoint.
Dial Mode	How the participant joined the call. Possible values include: <ul style="list-style-type: none"> Audio or Video Dial-In Audio or Video Dial-Out
Bridge	The MCU on which the participant's call resides.


3 Use these conference actions as needed:

Action	Use this action to...
Copy  .	Schedule a new conference that duplicates the selected conference settings.
View	View information for the selected conference.
Terminate  .	End an active conference.
Extend Duration  .	Extend the duration of an active conference.

Action	Use this action to...
Change Layout 	<p>For applicable endpoints.</p> <p>Change the default video layout for the conference display.</p> <ul style="list-style-type: none"> Switching.  Indicates that the display changes each time the speaker changes, and everyone sees the current speaker. Select a Frame Count, then select the specific layout for the frames. <p>The available layouts are Continuous Presence settings.</p>
Add Participant	Add one or more participants to the selected conference.
Add Guest	Add a guest to the selected conference.
Add Room	Add one or more rooms to the selected conference.
Add Favorites	Add participants from one of your Favorites lists to the selected conference.
Join Conference	Join the conference, monitor the conference, and talk with participants as needed.

4 Use these participant actions as needed:

Action	Use this action to...
Mute  or Unmute Audio 	Mute or unmute the selected participant's audio line into the conference. This option appears only when the conference is running on an external MCU. The Audio column in the Participants list shows the current status of this setting.
Block  or Unblock Video 	Block or unblock the selected participant's video line into the conference. This option appears only when the conference is running on an external MCU. The Video column in the Participants list shows the current status of this setting.
Connect  or Disconnect 	Disconnect or reconnect the selected participant to the conference. A disconnected participant is still associated with the conference and cannot be scheduled for other conferences.
Remove 	Remove the selected participant from the Participants list at which time the participant can be scheduled for another conference.
Send Message 	Send a message to the selected participant's registered Polycom endpoint. The message appears briefly on the monitor for the selected video endpoint.

Action	Use this action to...
Acknowledge Help 	Acknowledge a request for help and send a message to the requesting endpoint.
Manage Device	Open the web-based user interface for the selected participant's endpoint in a new browser window.
Save as Favorite	Function available when the selected participant has an associated endpoint to which the system can dial out. Save the selected participant to an existing Favorites List.
Connect All New	Function available only when the system is displaying the New Conference Participants list. Initiates the system dial out to new participants.

Add Additional Participants to an Active Conference



Operators can add additional participants to an active conference.



Note

Dial Out is the only **Dial Option** the system allows for adding participants to an active conferences.

To add additional conference participants to an active conference

- 1 Go to **Conference > Ongoing**.
- 2 From the list of **All Conferences**, select the conference of interest and click **Manage** .
- 3 To add participants from the local directory or enterprise directory:
 - a Click **Add Participant** .
 - b Enter all or part of a participant's **Last Name** or **First Name** into the appropriate field and click **Search**.

A list appears of participant's names that meet the search criteria.




Notes

- Depending on the search domain, the search function may return different results. See **"Filter and Search a List"** on page 4.
- The search results only include users associated with endpoints.

- c Select the participant's name from the list.
The participant's name appears in the underlying **New Conference Participants** list.
 - d Repeat steps a through c to add all domain participants and then click **Close**.
 - e If necessary, edit the new participants' settings. See ["Edit a Participant's Settings"](#) on page 57.
- 4 To add participants from the **Guest Book**:
 - a Click **Add Guest**.
 - b From the **Guest Book** dialog box, select the guest's name from the list.
The guest's name appears in the underlying **New Conference Participants** list.
 - c Repeat step b to add all guest participants and then click **Close**.
 - 5 To add new guest participants (participants not available from the local directory, enterprise directory, or **Guest Book**), see step 8 on page 51.
 - 6 To initiate the system dial out to new participants, select the participants of interest from the **New Conference Participants** list and click **Connect New Participants**.
The system dials out to the participants and adds them to the conference.

Add a Room to an Active Conference

To add a room to an active conference



- 1 Go to **Conference > Ongoing**.
- 2 From the list of **All Conferences**, select the conference of interest and click **Manage** .
- 3 From the **Conference Actions** list, click **Add Room**.
- 4 From the **Add Room** dialog box, select the site location of the room.
The list of conference rooms at the site appears.
- 5 Select the conference room of interest.
The conference room name appears in the underlying **New Conference Participants** list.
- 6 Click **Close**.

- 7 To initiate the system dial out to the room, select the room from the **New Conference Participants** list and click **Connect New Participants**.

The system dials out to the room endpoint system and adds the room to the conference.

View the Video of a Participant in an Active Conference


To view the video of a participant in an active conference

- 1 Go to **Conference > Ongoing**.
- 2 From the list of **All Conferences**, select the conference of interest and click **Manage** .
- 3 Select a participant from the **Participants** list.
The selected participant's video appears in the **Conference Image** section of the interface.
- 4 Click **Shuffle**  to shuffle to the next participant's video.

Join an Active Conference

By default, users assigned the **Operator** role can join an active conference to offer conference support.


To join an active conference

- 1 Go to **Conference > Ongoing**.
- 2 From the list of **All Conferences**, select the conference of interest and click **Manage** .
- 3 From the **Conference Actions** list, click **Join Conference**.
The **Join Conference** dialog box appears.
- 4 If the conference uses bridge cascading, select a bridge for the call into the conference.
- 5 If you have multiple endpoints, choose the endpoint to use to join the conference.
- 6 Click **Join Conference**.
Your endpoint is added to the conference with your video blocked but your audio not muted.

Add a Participant from a Favorites List to an Active Conference

By default, users assigned the **Operator** role can work with favorites lists.


To add a participant from a favorites list to an active conference

- 1 Go to **Conference > Ongoing**.
- 2 From the list of **All Conferences**, select the conference of interest and click **Manage** .
- 3 From the **Conference Actions** list, click **Add Favorites**.
- 4 From the **Favorites List**, expand the list of interest.
The names of the participants in the list is displayed.
- 5 Select the participant of interest from the list.
The participant's name appears in the underlying **New Conference Participants** list.
- 6 Repeat steps 4 and 5 to add all participants from the **Favorites List** and then click **Close**.
- 7 To initiate the system dial out to new participants, select the participants of interest from the **New Conference Participants** list and from the **New Participants Action** menu, click **Connect New Participants**.
The system dials out to the participants and adds them to the conference.

Add/Save a Participant to a Favorites List

By default, users assigned the **Operator** role can work with favorites lists.

To add or save a conference participant to a favorites list

- 1 Go to **Conference > Ongoing**.
- 2 From the list of **All Conferences**, select the conference of interest and click **Manage** .
- 3 From the **Participants** list, select the participant of interest.
- 4 From the **Participant Actions** menu, click **Save as Favorite**.
The names of the participants in the list is displayed.
- 5 From the **Save as Favorite Participant** dialog box, select the Favorite List to which to save the participant and click **OK**.



Manage a Participant's Endpoint During a Conference








The **Manage** page also allows operators to manage conference participant's endpoints.





- These context-sensitive commands only appear when the participant's endpoint supports the action.
- These commands work for rooms on the participant list as well.

To manage a participant's endpoint

- 1 Go to **Conference > Ongoing**.
 - 2 Select the conference of interest and click **Manage** .
- The **Participants** list appears.
- 3 To view participants geographically, click .
 - 4 Double-click on the participant of interest.
 - 5 Use these participant actions as needed. These actions are also available from the **View Participants Details** dialog box.


Action	Use this action to...
Mute  or Unmute Audio 	Mute or unmute the selected participant's audio line into the conference. This option appears only when the conference is running on an external MCU. The Audio column in the Participants list shows the current status of this setting.
Block  or Unblock Video 	Block or unblock the selected participant's video line into the conference. This option appears only when the conference is running on an external MCU. The Video column in the Participants list shows the current status of this setting.
Connect  or Disconnect 	Disconnect or reconnect the selected participant to the conference. A disconnected participant is still associated with the conference and cannot be scheduled for other conferences.
Remove 	Remove the selected participant from the Participants list at which time the participant can be scheduled for another conference.

Action	Use this action to...
Send Message 	Send a message to the selected participant's registered Polycom endpoint. The message appears briefly on the monitor for the selected video endpoint.
Acknowledge Help 	Acknowledge a request for help and send a message to the requesting endpoint.
Manage Device	Open the web-based user interface for the selected participant's endpoint in a new browser window.


View a Participant's Details During a Conference

This procedure describes how to view details for a participant's endpoint while it is in conference.

To view a participant's endpoint details

- 1 Go to **Conference > Ongoing**.
- 2 Select the conference of interest and click **Manage** .

The **Participants** list appears.



- 3 To view participants geographically, click .
- 4 Double-click on the participant of interest.

The **View Participant Details** dialog box appears with the **Call Properties** displayed. It includes the **Near End** and **Far End** video, the Participant's name, **Status**, **Errors**, **Warnings**, **Endpoint Type**, **Address**, **Access**, and **Bit Rate**.

It also includes a list of **Participant Actions**. For more information about these actions, see ["Manage a Participant's Endpoint During a Conference"](#) on page 76.

- 5 To view additional participant details, change the selection in the **Call Properties** drop-down menu.
 - If you select **Device**, you'll see these participant details:

Setting	Description
Endpoint Type	Usually the endpoint model, such as Polycom HDX system.
IP Address	The IP address for the endpoint.
Site	The location of the endpoint as identified by its IP address and the subnet of the site.

Setting	Description
Gatekeeper	The gatekeeper with which the endpoint is registered.
GDS	The Global Directory Service for the endpoint. Usually the Polycom Global Address Book.
Presence	Whether or not the endpoint is registered with a Presence service, so that its availability can be reported.
Device Managed	Whether or not the endpoint is registered with a Provisioning service, so that it can be configured automatically.
ISDN Line Status	<p>The status of the ISDN line. Possible values include:</p> <ul style="list-style-type: none"> Operational  Non-operations  <p>This field is blank for the following endpoint types: PVX, MGC, RMX, GW/MCU, Other, and TANDBERG.</p>
Alias Type	If the endpoint has an alias designation, the type of alias. Possible types include E.164, H.323 ID, URL, Transport Address, E-mail, Party Number, and Unknown.
Alias Value	Value for the alias type shown.

- If you select **Call Details**, you'll see these participant details:


Setting	Description
Video Protocol	<p>The video connection protocol, both transmission (Tx) and reception (Rx), the endpoint is using. Possible values include:</p> <ul style="list-style-type: none"> H.261 H.261 is an ITU standard designed for two-way communication over ISDN lines and supports data rates which are multiples of 64Kbit/s. H.261 supports CIF and QCIF resolutions. H.263 H.263 is based on H.261 with enhancements that improve video quality over modems. It supports CIF, QCIF, SQCIF, 4CIF and 16CIF resolutions. H.264
Video Format	The video format, both transmission (Tx) and reception (Rx), the endpoint is using.
Video Rate	The video bandwidth negotiated with the far site.
Video Rate Used	The actual video bandwidth used in the call to the far site.

Setting	Description
Video Frame Rate	Specifies the frame rate to use.
Video FEC Errors	The number of Forward Error Correction (FEC) errors that have been corrected in the current call.
Cause Code	
Audio Rate	The audio bandwidth negotiated with the far site
Audio Protocol	The audio connection protocol, both transmission (Tx) and reception (Rx), the endpoint is using.

- If you select **Call Quality of Service**, you'll see these standard service measurements: **Total Packet Loss**, **% Packet Loss**, **Audio Packet Loss**, **Video Packet Loss**, **Audio Jitter**, and **Video Jitter**.

Terminate an Active Conference


To terminate an active conference

- 1 Go to **Conference > Ongoing**.
- 2 Select the conference of interest and click **Terminate** .
- 3 Click **Terminate** to confirm the termination.

Delete a Conference

Users can delete future or past conferences. Users cannot delete active conferences.

To delete a conference

- 1 Go to **Conference > Future**.
- 2 To delete a past conference, select the appropriate filter (such as **Yesterday Plus**).
- 3 Select the conference of interest and click **Delete** .
- 4 If you select a recurring conference, a dialog box appears asking you if you want to delete just the conference you selected or all conferences in the series. Make the appropriate choice. Active conferences in the series cannot be deleted.

5 Click **Delete** to confirm the deletion.


The conference is deleted. For future conferences, the system E-mails the change to the conference owner and participants and releases the participant and room resources.

Conference and Participant Details

This chapter lists the conference and participant detail fields for reference. It includes:

- [Conference Details](#)
- [Conference Features](#)
- [Bridge \(MCU\) Features](#)
- [Participants List](#)
- [Participant Details](#)
- [Participant Settings](#)

Conference Image

The Conference Image section displays the selected participant's video. **Shuffle**  to shuffle to the next participant's video

Conference Details

The **Conference Details** section has these fields.

Section	Description
Owner	The name of the person who created the conference. Schedulers only see the conferences they own. Not applicable for ad hoc conferences.
Start Date/Time	For a scheduled conference, the start date and time of the conference and the time difference between the local time and the standard time. For an unscheduled conference, the date and time the conference started.

Section	Description
Duration	For a scheduled conference, how long the conference is scheduled to last. For a completed conference, how long the conference actually lasted.
End Date/Time	The date and time the conference ended
Type	The type of conference. Possible values include: <ul style="list-style-type: none"> Audio Audio-Video
Status	The state of the conference. Possible values include: <ul style="list-style-type: none"> Active Declined Finished Future
Recurring	Whether or not the conference was scheduled as a recurring conference
Connection	Connection information about the conference. Possible values include: <ul style="list-style-type: none"> Multipoint Point To Point Gateway
Bit Rate	The rate (in kbps) at which to transfer the conference audio or video data
Schedule ID	System-assigned ID used for troubleshooting
Conf Monitoring ID	System-assigned ID used for troubleshooting
Video Layout	The video layout for the conference: Video Switching or Continuous.
Video Format	For a conference hosted on an MCU, the video format of the conference data stream. Possible values include: <ul style="list-style-type: none"> Auto CIF QCIF 4CIF 16CIF VGA SVGA XGA NTSC
Video Protocol	For a conference hosted on an MCU, the video protocol of the conference data stream. Possible values include: <ul style="list-style-type: none"> Auto H.261 H.263 H.264

Section	Description
Audio Algorithm	<p>For a conference hosted on an MCU, the audio compression ratio of the conference data stream. Possible values are:</p> <ul style="list-style-type: none"> AUTO G.711 G.722 Siren 7 (16 kbps)

Conference Features

The **Conference Features** section has these fields.

Section	Description
Conference Passcode	The conference passcode, which is assigned either by the system or the scheduler.
Chairperson Option	<p>Indicates whether or not the conference requires a chairperson.</p> <p>Note</p> <p>The RMX 1000 system does not support the Chairperson feature.</p>
Chairperson Passcode	The passcode the chairperson must enter to take control of the conference. Not applicable when no chairperson is designated.
Chairperson	The name of the chairperson. Not applicable when no chairperson is designated.
Lecture Mode	<p>The type of Lecture Mode, if any, that was selected when the conference was created. Possible values are None, Lecture, and Presentation.</p> <p>Note</p> <p>The RMX 1000 system does not support Lecture Mode.</p>
Lecturer	The name of the lecturer. Not applicable when Lecture Mode is None .
Lecture View Switching	Indicates whether or not automatic switching between participants is enabled.
Dual Stream Mode	<p>Possible values are:</p> <ul style="list-style-type: none"> None People+Content Visual Concert PC Visual Concert FX Duo Video Unknown

Section	Description
T120 Rate	<p>Possible values are:</p> <ul style="list-style-type: none"> • None • HMLP - Var • HMLP - 384 • HMLP - 320 • HMLP - 256 • HMLP - 192 • HMLP - 128 • HMLP - 6.4 • HMLP - 62.4 • HMLP - 14.4 • MLP - Var • MLP - 64.4 • MLP - 62.4 • MLP - 46.4 • MLP - 40 • MLP - 38.4 • MLP - 32 • MLP - 30.4 • MLP - 24 • MLP - 22.4 • MLP - 16 • MLP - 14.4 • MLP - 6.4 • MLP - 4
End Time Alert	Whether or not the system alerts participants to the end of the conference by playing an end tone
Entry Tone	Whether or not an entry tone is played to all connected participants when a participant joins the conference
Exit Tone	Whether or not an exit tone is played to all connected participants when a participant disconnects from the conference

Bridge (MCU) Features

The **Bridge (MCU) Features** section, which applies only for conferences that use an MCU, has these fields.

Section	Description
MCU Name	The MCU device name hosting the conference. Not applicable when the conference is not being hosted on an MCU.
Numeric ID	The unique conference identifier assigned by the MCU
Entry Queue Access	<p>Whether or not the conference has an entry queue enabled</p> <p>Note</p> <p>The CMA system enables entry queues on a per MGC basis and all conferences on an entry queue enabled MGC will be scheduled with entry queue access.</p>

Section	Description
Meet Me per Conf	Whether or not the a conference is a Meet Me conference, for which a dial-in number is assigned, so that undefined participants can connect to the conference
Conference on Port	(MGC only) Indicates whether or not the MGC is set to Conference on Port, which conserves bandwidth and ports. In this case, all participants are on a single video port and use the same connection speed and video format.
Message Service Type	Displays the type of messages participants joining the conference hear. Possible values are: <ul style="list-style-type: none"> • None • Welcome (No wait) • Attended (Wait) • IVR
Message Service Name	Name on the MCU of the Message Service. So, for example, a service name IVR70 which provides the IVR service

Participants List

The **Participants** section has these fields.

Section	Description
Name	The participant's name
Call Info	How the participant joined the call. Possible values include: <ul style="list-style-type: none"> • Video Dial-Out • Audio Dial-In@<Address> • Video Dial-In@<Address> • In Person • Room Only

Participant Details

The **Participant Details** section has these fields.

Section	Description
Name	The participant's name
Type	The type of conference connection. Possible values include: <ul style="list-style-type: none">• Audio Only• Audio-Video• Other (for In Person and Room Only participants)
Endpoint Name	The name assigned to the participant's endpoint when added to the system
Connection Status	The state of the participant's endpoint connection. Possible values include: <ul style="list-style-type: none">• Connected• Connecting• Declined• Disconnected• Disconnecting• Error• Unknown
Interface Type	The interface protocol of the participant's endpoint. Possible values include: <ul style="list-style-type: none">• IP• ISDN
Number	The IP address or phone number of the participant's endpoint (if a dial-out) or the participant's port address on the MCU (if a dial-in)
Bit Rate	The audio or video data transfer rate (in kbps) of the participant's endpoint

Participant Settings

The **Participant Settings** dialog box has these fields.

Section	Description
Name	The participant's name.
Endpoints	The participant's managed endpoint(s) if available.
Email	The participant's E-mail address (ASCII only) for participants or guests without managed endpoints.
Type	The type of participant. Possible values include: <ul style="list-style-type: none"> • Domain User • Local User • Domain Resource (a room) • Local Resource (a room) • Guest
How will this participant join the conference?	How the participant will join the conference. Possible values include: <ul style="list-style-type: none"> • In Person (requires no dial settings) • Room Only • Audio Only (Dial in) • Use Video
Bit Rate	The audio or video data transfer rate (in kbps) of the participant's endpoint.
Dial Options	Available only if the participant is joining via a video endpoint system. Possible values include: <ul style="list-style-type: none"> • Dial-In • Dial-Out
Dial Type	The protocol the audio or video endpoint system uses. Select E.164, H323, IP (SIP IRI), or Annex-O. If no dial type is selected, it defaults to E.164.

If you select a **Dial Option** of **Dial-Out** for a participant without a managed endpoint, the **Participant Settings** dialog box has these additional fields.

Section	Description
Number	(H.323 and H.320 dial types) The participant's phone number
Extension	The specific dial string for the participant.
MCU Service	MCU service defined on the MCUs that the CMA system has registered.

Section	Description
Country	(H.320 dial type only) The country to which the system will dial out to the participant
Area/City Code	(H.320 dial type only) The area code to which the system will dial out to the participant
Use Modified Dial Number	(H.320 dial type only) Click this check box to add a specific prefix to the participant's phone number. The Number field becomes active
Number	(H.320 dial type only) The complete modified dial number as required to include PBX exit codes, dialing prefixes, or other installation-specific dial string requirements.
SIP URI	SIP dial type only) The SIP URI the MCU must resolve to contact the participant.

Endpoint Management Overview

This chapter provides an overview of the Polycom® Converged Management Application™ (CMA®) system's endpoint management functions. It includes these topics:

- [Endpoint Menu, Views, and Lists](#)
- [Endpoint Types](#)
- [Endpoint Configuration/Provisioning](#)
- [Endpoint Gatekeeper Registration Policies](#)
- [Endpoint Software Updates](#)
- [Endpoint Passwords](#)
- [Considerations for Third-Party Endpoints](#)


Endpoint Menu, Views, and Lists

The CMA system **Endpoint** menu provides these views of the **Endpoint** list:

- **Monitor View** – Displays the list of all registered and managed endpoints. Use this view to monitor and manage endpoints. See [“Monitor View”](#) on page 90.
- **Peripherals View** – Displays the list of all peripherals connected to managed endpoints. Use this view to see the status of peripherals. See [“Peripherals View”](#) on page 93.
- **Bundled Provisioning** – Displays the list of available endpoint provisioning bundles. See [“Bundled Provisioning View”](#) on page 95.
- **Automatic Provisioning** – Displays the list of dynamically managed endpoints eligible for automatic provisioning. See [“Automatic Provisioning View”](#) on page 96.
- **Scheduled Provisioning** – Displays the list of standardly managed endpoints eligible for scheduled provisioning. See [“Scheduled Provisioning View”](#) on page 97.

- **Automatic Software Update** – Displays the list of dynamically managed endpoints eligible for automatic software updates. See [“Automatic Software Update View”](#) on page 99.
- **Scheduled Software Update** – Displays the list of standardly managed endpoints eligible for scheduled software updates. See [“Scheduled Software Update View”](#) on page 101.

All of the **Endpoint** views have the following information:

Section	Description
Views	The views you can access from the page.
Actions	The set of available commands. The constant command in the Endpoint views is Refresh  , which updates the display with current information.
Endpoint List	The context-sensitive Endpoint list for the selected view.
Device Information	Information about the endpoint selected in the endpoint list including: <ul style="list-style-type: none"> • “Device Summary Information” on page 213 • “Device Status Information” on page 215 • “Call Information” on page 217 • “Device Alerts Information” on page 218 • “Provisioning Details” on page 218 • “Software Update Details” on page 219











Monitor View

Use the **Endpoint Monitor View** to monitor and manage endpoints.

Endpoint List in the Monitor View

By default the **Endpoint** list in the **Monitor View** displays a list of all endpoints that registered automatically with the CMA system gatekeeper and endpoints that were added manually for management and monitoring purposes.








The **Endpoint** list in this view has these fields.



Field	Description
Filter	<p>Use the filter choices to display other views of the Endpoint list, which include:</p> <ul style="list-style-type: none"> • Type - Filters the list by type. For more information, see “Endpoint Types” on page 103. • Alerts - Filters the list by alert type: Help, Error, or Warning. • Connection Status - Filters the list by connection status: In a Call, Online, or Offline. • Name - Filters the list by system name entered. • IP Address - Filters the list by IP address entered. • Dial String - Filters the list by dial string (SIP, H.323, or ISDN) entered. • Site - Filters the list by site location entered. • Area - (Available only when Areas are enabled.) Filters the list by the area with which the endpoint is associated. • VIP - Filters the list for VIP endpoints.
Status	<p>The state of the endpoint. Possible values include:</p> <ul style="list-style-type: none"> • Online  • Offline  • In a call  • Gatekeeper registered  • Signalling unregistered  • Error  • All paired peripherals are connected without alerts  • One or more paired peripherals are turned off or no longer connected  • One or more paired peripherals has an error 
Mode	<p>The management mode for the endpoint. Possible values include:</p> <ul style="list-style-type: none"> • Dynamic management mode  • Standard management mode (no icon) <p>For a description of these modes, see “Endpoint Configuration/Provisioning” on page 105.</p>
Name	The assigned name of the endpoint.
Model	The type of endpoint. For valid endpoint types, see “Endpoint Types” on page 103.
IP Address	The IP address assigned to the endpoint.
Area	(Available only when Areas are enabled.) The area with which the endpoint is associated.

Field	Description
Dial String	The dial string for the endpoint. If the endpoint has more than one dial string, it displays one based on this order: <ul style="list-style-type: none"> • SIP • H.323 • ISDN
Site	The site to which the endpoint belongs.
Owner	The user associated with the endpoint.

Actions in the Monitor View

Besides providing access to the endpoint views, the **Actions** section of the **Monitor View** may also include these context-sensitive commands depending on the selected endpoint type.

Action	Use this action to...
Available for all endpoint types	
Add 	Manually add an endpoint to the CMA system or find a endpoint on the network.
View Details 	Display all of the Device Details for the selected endpoint.
Edit 	Change connection settings for the selected endpoint. Note that if this is a managed endpoint, the endpoint may overwrite settings entered manually.
Delete 	Delete the selected endpoints.
Search Devices	Search the list of endpoints by IP range. Searching by IP range will not include endpoints that are dynamically-managed.
Available for only selected endpoint types	
Manage 	Open the selected endpoint's management interface in a separate browser window. This command is not available for the following endpoint types: iPower , PVX , and Other .
Send Message 	Send a text message (ASCII only, 100 characters maximum) to the selected endpoint's video monitor. This command is not available for the following endpoint types: TANDBERG , iPower , and Other .
Clear Help 	Clear help for the selected endpoint on the CMA system.

Action	Use this action to...
Reboot Device 	Reboot the selected endpoint. This command is only available for HDX-Series , RealPresence Group Series , V-Series and VSX-Series endpoints with a Connection Status of Online .
Search Devices	Allows you to search for endpoints within a range of IP addresses. The results message displays the number of endpoints searched and the number of endpoints found within the IP range.
Manage Owner 	Edit information for the user (owner) of the selected endpoint. This command is applicable only when a user is associated with the endpoint.
View Peripherals	View information about peripherals. This command is only available when one or more peripherals is connected to an HDX-Series or RealPresence Group Series endpoint.
Associate User	Manually associate a user with the selected endpoint.
Associate Area	(Available only when Areas are enabled.) Associate the selected endpoint to an area so that only specified users can manage it.

For information about these endpoint actions, see [“Endpoint and Peripheral Management Operations”](#) on page 165.




Peripherals View

Use the **Peripherals View** to monitor peripherals connected to dynamically managed endpoints.

Peripherals List in the Peripherals View

By default, the **Peripherals** list displays a list of all peripherals that are connected or have been connected to endpoints managed by the CMA system.

The **Peripherals** list in this view has these fields.

Field	Description
Filter	Use the filter choices to display other views of the Endpoint list, which include: <ul style="list-style-type: none"> • Type - Filters the list by type. For more information, see “Endpoint Configuration/Provisioning” on page 105. • Paired Endpoint- Filters the list by the HDX or RealPresence Group Series to which the peripherals are connected. • IP Address - Filters the list by IP address entered. • Hardware Version - Filters the list by hardware version entered. • Software Version - Filters the list by software version entered.
Status	The state of the peripheral. Possible values include: <ul style="list-style-type: none"> • Connected  - Peripheral is connected to the endpoint. • Disconnected  - Peripheral is turned off or no longer connected to the endpoint. • Error  - Endpoint reports an error with the peripheral. • Blank - Endpoint is not reporting that the peripheral is connected.
Paired Endpoint	Name of the endpoint to which the peripheral is connected or Not Paired . The Not Paired designation means the peripheral was connected to an endpoint, but it is not connected to one now.
Type	The type of peripheral.
Serial Number	The serial number of the peripheral.
IP Address	The IP address assigned to the peripheral, if applicable.
Area	(Available only when Areas are enabled.) The area with which peripheral is associated. The peripheral inherits its area from the endpoint to which the peripheral is connected.
Hardware Version	The hardware version of the peripheral.
Software Version	The software version of the peripheral.

Actions in the Peripheral View

Besides providing access to the peripherals, the **Actions** section of the **Peripheral View** may also include these context-sensitive commands depending on the selected peripheral type and its status.

Action	Use this action to...
Delete Peripheral	(Available only when the peripheral is no longer paired with an endpoint.) Delete the peripheral from the Peripheral View list.
Display Applications	(Available only for peripherals on which you can install multiple applications.) Display a list of installed applications and their version.

Bundled Provisioning View

Use the **Bundled Provisioning View** to see the list of provisioning bundles available to dynamically managed HDX and RealPresence Group Series systems.

Endpoint List in the Bundled Provisioning View

By default, the **Bundled Provisioning View** displays the list of provisioning bundles available for use by dynamically-managed HDX or RealPresence Group Series systems.

The bundle list in the **Bundled Provisioning View** has the following information.

Field	Description
Filter	The filter choices for provisioning bundles that have been downloaded to the system. Possible values include: <ul style="list-style-type: none"> Name—Filters by the name of the provisioning bundle. Model—Filters by the endpoint type. Creation Date—Filters by the date the provisioning bundle was downloaded and created on the system. Description—Filters by the description of the provisioning bundle.
Name	The name assigned to the provisioning bundle when it was downloaded and created on the system.
Model	The exact type of endpoint to which the provisioning bundle applies as defined when it was downloaded and created on the system.
Creation Date	The date the provisioning bundle was downloaded and created on the system.
Description	The description assigned to the provisioning bundle when it was downloaded and created on the system.

Actions in the Bundled Provisioning View

The **Actions** section of the **Bundled Provisioning View** may include these context-sensitive commands.

Action	Use this action to...
Download	Create a new provisioning bundle by downloading the bundle from an HDX or RealPresence Group Series system on the network.
Delete	Delete the selected bundled from the bundle list.

Automatic Provisioning View

Use the **Automatic Provisioning View** to see the list of endpoints that are registered to the system for automatic provisioning.

Endpoint List in the Automatic Provisioning View

By default the endpoint list in the **Automatic Provisioning View** displays the list of Polycom HDX and RealPresence Group Series system endpoints registered to the CMA system for automatic provisioning.

The endpoint list in the **Automatic Provisioning View** has the following information.

Field	Description
Filter	<p>The filter choice for endpoint types that can be automatically provisioned. Possible values include:</p> <ul style="list-style-type: none"> • All—Displays all dynamically managed endpoint systems registered to the system. • HDX Series—Displays just the HDX endpoints registered to the system and deployed in dynamic management mode. • CMA Desktop—Displays just the CMA Desktop clients registered to the system. • VVX—Displays just the VVX systems registered to the system. • RealPresence Mobile—Displays just the RealPresence Mobile clients registered to the system. • RealPresence Group Series —Displays just the RealPresence Group Series endpoints registered to the system. • RealPresence Desktop—Displays just the registered RealPresence Desktop clients registered to the system.

Field	Description
Status	The status of the endpoint's last provisioning process. Possible values include: <ul style="list-style-type: none"> • Success • Failed • Clear
Name	The assigned name of the endpoint. Note The system assigns Polycom CMA Desktop systems a user name of <i>LastName_Firstname_CMADesktop</i> .
Type	The type of endpoint. Automatic provisioning is only available for the endpoint types listed in this table as Filter selections.
IP Address	The IP address assigned to the endpoint.
Area	The assigned Area associated with the endpoint, if any.
Last	The date and time of the endpoint's last provisioning. Note CMA Desktop clients are provisioned at the start of each session.

Actions in the Automatic Provisioning View

Because automatic provisioning is managed by the endpoint, there are no context-sensitive commands available in the **Automatic Provisioning View**.

Scheduled Provisioning View

Use the **Scheduled Provisioning View** to:

- View the list of endpoints that are eligible for scheduled provisioning
- Schedule one or more endpoints for provisioning
- Cancel a scheduled provisioning

Endpoint List in the Scheduled Provisioning View




By default, the endpoint list in the **Scheduled Provisioning View** displays the list of Polycom HDX system endpoints registered to the CMA system that are eligible for scheduled provisioning.

The **Endpoint** list in this view has the following information.

Field	Description
Filter	<p>The filter choice for endpoint types that can be scheduled for provisioning. Possible values include:</p> <ul style="list-style-type: none"> • HDX Series—Displays the Polycom HDX systems operating in standard management mode. • LifeSize® • QDX Series • TANDBERG T150 • TANDBERG C-Series • TANDBERG MXP • V and VSX Series • Viewstation • Viewstation FX & EX
Status	<p>The status of the endpoint's last provisioning process. Possible values include:</p> <ul style="list-style-type: none"> • Success • Pending • Failed • Clear
Name	The system name of the endpoint.
Type	The type of endpoint. Scheduled provisioning is only available for the endpoints types listed in this table as Filter selections.
IP Address	The IP address assigned to the endpoint.
Last	The date and time of the endpoint's last provisioning, unless its status has been cleared.
Pending	When the endpoint is scheduled for provisioning, this field shows the provisioning profile to be used for the scheduled provisioning process.
Scheduled	When the endpoint is scheduled for provisioning, this field shows the date and time for the next scheduled provisioning process.

Actions in the Scheduled Provisioning View

Besides providing access to the endpoint views, the **Actions** section of the **Scheduled Provisioning View** also includes these commands:

Action	Use this action to...
Provision 	Schedule provisioning for the selected endpoint(s).
Cancel Provision 	Cancel a previously scheduled provisioning operation.
Clear Status 	Change the status column for an endpoint to the Clear state.

You can perform these operations on multiple endpoints at the same time. To select multiple endpoints, hold the control key while you select the endpoints.

For information about these endpoint actions, see [“Endpoint Provisioning Operations”](#) on page 181.

Automatic Software Update View

Use the **Automatic Software Update View**, available from the **Endpoint** menu, to view the list of endpoints that have registered to the system for automatic software updates.

Endpoint List in the Automatic Software Update View

By default, the **Endpoint** list in the **Automatic Software Update View** displays all endpoints eligible for automatic software update. It has the following information.

Field	Description
Filter	Filter choices for this view include: <ul style="list-style-type: none"> • Type—Filters the list by endpoint type. • Name—Searches the list by the endpoint's system name. • IP Address—Searches the endpoint list by IP address. • ISDN Video Number—Searches the endpoint list by ISDN video number. • Dial String— Searches the endpoint list by dial string (SIP, H.323, or ISDN). • Site—Searches the endpoint list by site location.
Status	The status of the endpoint's last software update. Possible values include: <ul style="list-style-type: none"> • Success • Failed • Clear
Name	The system name of the endpoint.

Field	Description
Type	<p>The type of endpoint. Automatic software update is only available for these endpoint types:</p> <ul style="list-style-type: none">• All—Displays all dynamically managed endpoints together.• CMA Desktop—Displays just the Polycom CMA Desktop clients.• HDX Series—Displays just the Polycom HDX endpoints deployed in dynamic management mode.• VVX—Displays just the Polycom VVX systems.• Group Series—Displays just the Polycom RealPresence Group Series endpoints.
IP Address	The IP address assigned to the endpoint.
Current Version	The version of software installed during the last successful software update procedure.

Actions in the Automatic Software Update View

Because automatic (pull) software update is managed by the endpoint, there are no actions available in the **Automatic Software Update View**.

Scheduled Software Update View

Use the **Scheduled Software Update View**, available from the **Endpoint** menu, to:

- View the list of endpoints that are eligible for a scheduled software update
- Schedule one or more endpoints for a software update
- Cancel a software update.

Endpoint List in the Scheduled Software Update View

By default, the **Endpoint** list in the **Scheduled Software Update View** displays all endpoints eligible for scheduled software update.




The **Endpoint** list in the **Scheduled Software Update View** has the following information.

Field	Description
Filter	Filter choices for this view include: <ul style="list-style-type: none">• Type—Filters the list by endpoint type.• Name—Searches the list by the endpoint's system name.• IP Address—Searches the list by endpoint's IP address.• ISDN Video Number—Searches the list by endpoint's ISDN video number.• Alias—Searches the list by endpoint's alias.• Site—Searches the list by site location.
Status	The status of the endpoint's last scheduled software update. Possible values include: <ul style="list-style-type: none">• Success• Failed• Clear
Name	The system name of the endpoint.

Field	Description
Model	<p>The type of endpoint. Scheduled software update is only available for these endpoint types:</p> <ul style="list-style-type: none"> • HDX Series—Displays the Polycom HDX endpoints operating in standard management mode. • LifeSize® • QDX Series • TANDBERG T150 • TANDBERG C-Series • TANDBERG MXP • V and VSX Series • Viewstation • Viewstation FX & EX
IP Address	The IP address assigned to the endpoint.
Current Version	The version of software installed during the last successful software update procedure.
Scheduled	When the endpoint is scheduled for software update, this field shows the date and time for the scheduled software update process.

Scheduled Software Update View Actions

Besides providing access to the endpoint views, the **Action** section for the **Scheduled Software Update View** will also include these actions:

Action	Use this action to...
Software Update 	Schedule software update for the selected endpoints.
Cancel Update 	Cancel a scheduled or in progress software update operation.
Clear Status 	Change the status column for an endpoint to the Clear state.

For information about these endpoint actions, see “[Endpoint Software Update Operations](#)” on page 191.

Endpoint Types

The following tables describe the CMA system support for endpoints based on endpoint type and category of support. See the *Polycom CMA System Release Notes* for more information on tested and supported endpoint versions.

Polycom Endpoint Types	Gatekeeper Registration	Global Address Book Access	Dynamic Management ^a	Standard Management ^a	Scheduling (Dial In only) ^b	Scheduling (Dial In and Dial Out) ^b	Monitoring (Standard) ^c	Command and Control ^d	Reports for IP Calls ^e	Reports for ISDN Calls ^e	Supported Behind a Firewall ^f
CMA Desktop	Y	N	Y	N	Y	N	Y	N	Y	Y	Y
HDX Series (dynamic management mode)	Y	N	Y	N	N	Y	Y	Y	Y	Y	Y
HDX Series (standard management mode)	Y	Y	N	Y	N	Y	Y	Y	Y	Y	N
VVX Series	Y	N	Y	N	Y	N	Y	N	Y	N	Y
ViewStation Series	Y	Y	N	Y	N	Y	Y	Y	Y	N	N
ViewStation FX and EX Series	Y	Y	N	Y	N	Y	Y	Y	Y	N	N
V and VSX Series	Y	Y	N	Y	N	Y	Y	Y	Y	Y	N
QDX Series	Y	Y	N	Y	N	Y	Y	Y	Y	Y	N
PVX	Y	Y	N	N	Y	N	Y	N	Y	N	N
RealPresence Group Series	Y	Y	Y	N	N	Y	Y	Y	Y	N	Y
RealPresence Desktop	Y	N	Y	N	Y	N	Y	N	Y	N	Y
RealPresence Mobile	Y	N	Y	N	N	Y	Y	N	Y	N	Y

- Dynamic Management and Standard Management are mutually exclusive functionality.
- Scheduling (Dial In Only) and Scheduling (Dial In and Dial Out) are presented as mutually exclusive functionality. Some endpoints, such as Polycom VVX systems do not have interfaces that can be ask to perform dialing. Some endpoints, such as CMA Desktop clients and VVX systems require external MCU resources for dial-in conferences.
- Standard CMA monitoring does not involve using SNMP. It includes endpoint monitoring (online/offline status) and alerts.
- Command and Control means the CMA system can send a command like Send Message and Reboot, and the endpoint can receive and act on the command.

- e. Reports for IP Calls are generated as part of standard gatekeeper functionality. Reports for ISDN Calls are additional system functionality. Endpoints that aren't registered with the gatekeeper or ISDN calls send an alert to the device management function to record CDR information. Some legacy endpoints do not send this alert so the CDRs are not written.
- f. Supported behind a Polycom VBP device with Access Proxy enabled.

Endpoint Type	Gatekeeper Registration	Dynamic Management ^a	Standard Management ^a	Scheduling (Dial In only) ^b	Scheduling (Dial in and Dial out) ^b	Monitoring (Standard) ^c	Command and Control ^d	Reports for IP Calls ^e	Reports for ISDN Calls ^e
TANDBERG 150 MXP	Y	N	Y	N	Y	Y	Y	Y	N
TANDBERG 990/880/770 MXP	Y	N	Y	N	Y	Y	Y	Y	Y
TANDBERG C Series and Other TANDBERG Models	Y	N	Y	Y	N	Y	N	Y	N
LifeSize Team and Express 200	Y	N	Y	N	Y	Y	Y	Y	Y
Other LifeSize Models	Y	N	N	Y	N	N	N	Y	N
Other third-party endpoints: <ul style="list-style-type: none"> • Sony PCS • Aertha Maia Starr • VCON (Galaxy and Vigo) • VTEL 	Y	N	N	Y	N	N	N	Y	N

- a. Dynamic Management and Standard Management are mutually exclusive functionality.
- b. Scheduling (Dial In Only) and Scheduling (Dial In and Dial Out) are presented as mutually exclusive functionality.
- c. Standard CMA monitoring does not involve using SNMP. It includes endpoint monitoring (online/offline status) and alerts.
- d. Command and Control means the CMA system can send a Reboot command, and the endpoint can receive and act on the command.
- e. Reports for IP Calls are generated as part of standard gatekeeper functionality.

Some notes about the TANDBERG connection to the Global Address Book:

- TANDBERG endpoints do not need to register with the CMA system gatekeeper to access the Global Address Book.
- Even if the Global Address Book is password protected, TANDBERG endpoints are not required to provide a password. They have unrestricted access to the Global Address Book.
- Any third-party endpoint, including TANDBERG endpoints, that are registered to the CMA system gatekeeper are displayed in the Global Address Book. In this case, endpoints are not filtered out based on capability.

A CMA system may also list an endpoint type of **Other**. The CMA system cannot manage endpoints with a type of **Other** and cannot direct these endpoints to initiate point-to-point calls. A scheduled point-to-point call between two endpoint systems with an endpoint type of **Other** requires the use of an MCU.



Note

The Polycom RealPresence Mobility and Telepresence M100 systems register as endpoint type of **Other**. As such, the CMA can schedule and perform limited monitoring of these systems.

Endpoint Configuration/Provisioning

Polycom endpoint systems can be configured in three ways:

- In the room by using the system's remote control to navigate the screens and enter information.
- From a remote location by using the system's web interface to navigate the screens and enter information.
- From a remote location by using a management system's web interface to provision configuration settings to the endpoint system. The CMA system is a management system that provisions configuration settings.

The CMA system can provision several types of endpoints. Endpoint provisioning, which requires provisioning profiles, allows an administrator to remotely configure multiple endpoints of the same type with a standard set of settings. This eliminates the need to configure each endpoint individually either through the hand-held remote or the endpoint's web interface.

The CMA system supports three types of endpoint provisioning: bundled, automatic, and scheduled. Enable endpoints for only one type of provisioning.



Note

Polycom recommends that all endpoints in a region (that is, a gatekeeper zone) be managed by a single management system.

For more information, see:

- [Bundled Provisioning](#)
- [Automatic Provisioning](#)
- [Scheduled Provisioning](#)

Provisioning Best Practices

To use the available provisioning options most effectively, we recommend the following:

- 1 For each site in the CMA system, configure the site provisioning details as needed for each site. See [“Add a Site”](#) on page 465.
- 2 On each HDX and RealPresence Group Series endpoint, configure the system settings that are available in bundled provisioning for that model. Then download the provisioning bundle for each HDX and RealPresence Group Series endpoint to the CMA system. See [“Bundled Provisioning”](#) on page 106.
- 3 If you need unique provisioning settings for one or more groups of users, create automatic provisioning profiles with those settings and apply them to the appropriate groups. See [“Automatic Provisioning”](#) on page 107 and [“Add a Local Group”](#) on page 268.

For example, you may want to set a higher bit rate for the executives of your organization or for conference rooms used for large video conferences. You can create a group for these users/rooms and give that group an automatic provisioning profile with a higher bit rate.

Bundled Provisioning

The CMA system supports a **Bundled Provisioning** model for dynamically managed HDX and RealPresence Group Series endpoints. With **Bundled Provisioning**, a CMA system administrator can download a provisioning bundle from any already configured HDX and RealPresence Group Series endpoints. Any dynamically-managed HDX and RealPresence Group Series endpoints of the same model will receive the provisioning bundle when it next polls the CMA system for new provisioning information.



Note

Some configuration settings on dynamically managed endpoints that the CMA system provisions are associated with the site where the endpoint system is located. Site provisioning takes precedence.

Bundled provisioning provides businesses with an efficient and effective way to provision HDX and RealPresence Group Series endpoints consistently across each model. HDX and RealPresence Group Series endpoint users with

administrative rights can still change the settings on an HDX and RealPresence Group Series endpoint after the provisioning bundle is applied. However, if a newer bundle is sent by the CMA system, it will overwrite the user's changes.

The HDX and RealPresence Group Series system parameters that may be provisioned in a bundle are limited to the following types:

- Camera configuration settings
- Monitor configuration settings
- Microphone configuration settings
- Security settings
- Home screen settings

How Bundled Provisioning Works

In dynamic management mode, when an HDX and a RealPresence Group Series system starts up and at designated intervals thereafter, it automatically polls for new provisioning information from the CMA system. If a provisioning bundle exists on the CMA system that matches the model of the polling HDX or RealPresence Group Series endpoint, the provisioning bundle is sent over a secure HTTPS connection.

Endpoints do not poll for provisioning information if they are in a call. They restart polling after the call ends.

Provisioning information is applied in the following order:

- 1 Bundled provisioning, if a bundle exists for the same model.
- 2 Automatic provisioning profile, if the endpoint is part of a group assigned a profile.
- 3 Site provisioning, which takes precedence.

For information about how to download a provisioning profile, see [“Download a Provisioning Bundle”](#) on page 182.

Automatic Provisioning

The CMA system is a gatekeeper; it manages video and audio endpoints. However, the system also manages users, because endpoints are only useful when they provide access to users.

Automatic provisioning, which controls the automatic configuration of dynamically managed endpoints and the management of its video resources, is also tied to users and groups. That's because some users and groups may require significantly more video resources than others.

**Note**

Some settings on dynamically managed endpoints that the CMA system provisions are associated with the site where the endpoint system is located. Site provisioning takes precedence.

Currently, automatic provisioning is available for:

- Polycom VVX systems deployed in dynamic management mode
- Polycom HDX systems deployed in dynamic management mode
- Polycom RealPresence Group Series systems
- RealPresence Desktop clients
- RealPresence Mobile clients
- Polycom CMA Desktop clients

**Note**

Polycom CMA Desktop provisioning occurs on a session by session basis.

How Automatic Provisioning Works

In dynamic management mode, when an endpoint starts up and at designated intervals thereafter, it automatically polls for new provisioning information from the CMA system. The provisioning information is sent in XML format over a secure HTTPS connection.

Endpoints do not poll for provisioning information if they are in a call. They restart polling after the call ends.

When you add an automatic provisioning profile, the CMA system immediately rolls it out. If it rolls it out first thing in the morning, people who need to attend a “start the day” conference will have to first wait for their endpoint to be provisioned. Better to implement profiles in the middle of the work day and then let the provisioning occur at the designated polling interval.

Provisioning information is applied in the following order:

- 1 Bundled provisioning, if one exists for the same model.
- 2 Automatic provisioning profile, if the endpoint is part of a group assigned a profile.
- 3 Site provisioning, which takes precedence.

Automatic Provisioning Profiles

Automatic provisioning is enabled at the endpoint, but the CMA system must have automatic provisioning profiles for both the endpoint and the site at which the endpoint resides. So to ensure out-of-box usability, the CMA system comes with Default Provisioning Profiles for both. However, you can edit these default profiles to meet your needs or add additional provisioning profiles to assign different video resources to different groups of users.



Notes

- If an automatic provisioning profile provisions a setting that the endpoint is not capable of fulfilling, the endpoint will ignore those settings.
- The name of the **Default Provisioning Profile** is stored in the system database and is not localized into other languages. If you wish to localized it into your language, edit the profile and give it a new profile name.

For information about how to add an automatic provisioning profile, see [“Add an Automatic Provisioning Profile”](#) on page 183.

The following table shows the fields you can configure when adding a new automatic provisioning profile. You may find more implementation details about these fields in the endpoint system documentation.

Field	For the endpoint systems being provisioned...
System Settings	
Language	Specifies the language for the video endpoint system's user interface. Possible values include: English, German, Spanish, French, and Chinese (Simplified Chinese only).
Allow Access to User Setup	Specifies whether the User Settings screen is accessible to users via the System screen. Select this option to allow endpoint system users to change limited environmental settings.
Allow Directory Changes	Specifies whether endpoint system users can save changes they make to the directory on contacts/favorites list.
Call Detail Report	<p>Specifies whether to collect call data for the Call Detail Report and Recent Calls list. When selected, information about calls can be viewed through the endpoint system's web interface and downloaded as a .csv file.</p> <p>Note</p> <p>If this setting is disabled, applications such as the CMA system or the Polycom Global Management System™ will not be able to retrieve Call Detail Report (CDR) records.</p>

Field	For the endpoint systems being provisioned...
Maximum Time in Call (minutes)	Specifies the maximum number of minutes allowed for a call. Enter 0 to remove any limit.
Recent Calls	<p>Specifies whether to display the Recent Calls button on the home screen. The Recent Calls screen lists the site number or name, the date and time, and whether the call was incoming or outgoing.</p> <p>Note</p> <p>If the Call Detail Report option is not selected, the Recent Calls option is not available.</p>
Screen Saver Wait Time	<p>Specifies how long the system remains awake during periods of inactivity. The default is 3 minutes. If the system requires users to log in, the screen saver timeout also logs out the current user.</p> <p>Setting this option to Off prevents the system from going to sleep. To prevent image burn-in, specify 3 minutes or less.</p>
Directory Search Mode	<p>Specifies how endpoint directory searches are initiated by the endpoint user. Possible values are:</p> <ul style="list-style-type: none"> Automatic—The search is executed after the user stops entering characters. Manual—The search is executed only when the user explicitly clicks the Search button.
Home Screen Settings	
Display Contact List as Home Screen	Specifies whether or not to display the contact list as the entry screen.
Display H.323 Extension	<p>Lets users placing a gateway call enter the H.323 extension separately from the gateway ID.</p> <p>If you do not select this setting, endpoint system users make gateway calls by entering the call information in this format:</p> <p><i>gateway ID + ## + extension</i></p>
Enable Availability Control	When enabled, lets users set their availability in the endpoint system's local user interface.
H.323 Settings	
Maximum Speed for Receiving Calls (kbps)	<p>Allows you to restrict the bandwidth used when receiving calls.</p> <p>If the far site attempts to call the endpoint system at a higher speed than selected here, the call is re-negotiated at the speed specified in this field.</p>

Field	For the endpoint systems being provisioned...
Preferred Speed for Placing Calls (kbps)	<p>Determines the speeds that will be used for calls from this endpoint system when:</p> <ul style="list-style-type: none"> The Call Quality selection is either unavailable or set to Auto on the Place a Call screen The call is placed from the directory <p>If the far-site endpoint system does not support the selected speed, the endpoint system automatically negotiates a lower speed.</p>
Call Settings	
Preferred Dialing Method	<p>Specifies the preferred method for dialing various call types.</p> <ul style="list-style-type: none"> If set to Auto, calls use the configured dialing order. If set to Manual, the endpoint systems will prompt the user to select the call type from a list when placing a call.
Audio Settings	
Mute Auto Answer Calls	Specifies whether or not to automatically mute incoming calls.
CMA Desktop Settings	
Allow IM/Chat	When enabled, specifies that the Polycom CMA Desktop client can initiate instant messaging.
Enable Screen Saver When in Call	
Calendaring Settings	
Enable Calendaring	When enabled, specifies that the CMA system will provision the endpoint for Polycom Conferencing for Outlook. This includes provisioning the Microsoft Exchange server and calendaring settings for the endpoint system.
Alert Tone	When enabled, specifies that an endpoint system provisioned for Polycom Conferencing for Outlook will play a sound along with the meeting reminder. In this case, the endpoint will only play a sound when the system is not in a call.
Display Private Meeting	When enabled, specifies that an endpoint system provisioned for Polycom Conferencing for Outlook will display details about meetings marked private.
Meeting Reminder Time	Specifies the number of minutes before the meeting an endpoint system provisioned for Polycom Conferencing for Outlook will display a reminder.

Field	For the endpoint systems being provisioned...
Microsoft Lync Settings	
Select method to find Server	<p>Specifies how the CMA system will locate the Lync server that it will provision to endpoints. Possible values are:</p> <ul style="list-style-type: none"> • Disable Integration—The CMA system will not provision a Lync or Office Communication Server. • DNS SRV Record—The CMA system will issue a DNS query to locate the Lync or Office Communication Server and provision that information to endpoints. • Server Name—The CMA system will use the specified Server Address. Enter the Lync or Office Communication Server address or DNS name.
Transport Protocol	<p>Specifies the transport protocol for communications with the Office Communications Server. Possible values are:</p> <p>Auto—The communication protocol will be auto-negotiated.</p> <p>TCP—This protocol has error-recovery services, message delivery is assured, and messages are delivered in the order they were sent.</p> <p>UDP—This protocol does not provide error-recovery services, message delivery is not assured, and messages are not necessarily delivered in the order they were sent.</p> <p>TLS—This protocol transfers communications over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection.</p>
Group Name	Specifies the group name for which the endpoint system should be provisioned.
VVX Settings	
Configuration Server URL	Specifies the IP address for the system that will provide provisioning service. All addresses can be followed by an optional directory and optional filename.
Logging Server URL	Specifies the directory to use for log files, if required. A URL can also be specified. This field is blank by default.
Configuration Data	Enter XML data for a custom configuration. Allows the CMA system administrators to provision settings that the CMA system does not normally provide.

Profile Order and Priority

Automatic provisioning profiles are associated with groups, but what about those users who belong to more than one group – what determines their experience? When you add new profiles, you assign a **Profile Order**. The **Profile Order** determines which provisioning profile takes priority.

Consider the following example:

- Jason Smith is part of the Support group and also part of the Executive group.
- The Support group is assigned an automatic provisioning profile named Low-Bandwidth, which allows a maximum speed for receiving calls of 128kbps.
- The Executive group is assigned an automatic provisioning profile called High-Bandwidth, which allows a maximum speed for receiving calls of 1920kbps
- The Low-Bandwidth profile is assigned a profile order of 1, while the High-Bandwidth profile is assigned a profile order of 2.

In this example, Jason's endpoint is provisioned with the Low-Bandwidth provisioning profile, because it has the higher priority.

So when you add provisioning profiles, you may want to assign provisioning profiles with more robust privileges a higher priority than those providing less privileges.

Scheduled Provisioning

Scheduled provisioning is enabled at the CMA system. To schedule an endpoint for provisioning, the CMA system must already have a scheduled provisioning profile created for the endpoint.

How Scheduled Provisioning Works

In this standard management mode, administrators with **System Setup** permissions can schedule provisioning for one endpoint or a group of endpoints; and they can schedule provisioning to occur immediately or for a date and time in the future. The provisioning data is sent in XML format over a secure HTTPS connection.

Scheduled provisioning is available for these endpoint types:

- ViewStation endpoints
- ViewStation FX & EX endpoints
- V and VSX Series endpoints
- Selected TANDBERG endpoints – TANDBERG 150, 990, 880, and 770 endpoints

- HDX Series--Polycom HDX systems deployed in standard management mode

Scheduled Provisioning Profiles

The CMA system does not include a default profile for scheduled provisioning. You must create a profile before you can schedule an endpoint for provisioning. Create a different profile for each endpoint type (Polycom HDX system or Polycom CMA Desktop) and group of users.

Some examples of when to use scheduled provisioning profiles follow.

- To apply a standard set of options to each new endpoint
By creating templates of standard settings for different types of endpoints, or for the needs of different users, you can have the CMA system apply all the settings at once. After the endpoint is connected and registered with the CMA system, you can use a provisioning profile that defines a range of other options.
- To update the password for all endpoints of a particular type
For security purposes, you can create a provisioning profile to update the password for endpoints on a regular basis and reuse the same profile quarterly. You might have several profiles, one for each type of endpoint to update.
- To change the IP address of the CMA system gatekeeper when the CMA system is moved

For information about how to add a scheduled provisioning profile, see [“Add a Scheduled Provisioning Profile”](#) on page 186.

Scheduled Provisioning of Polycom Endpoints

The following table shows the fields you can provision when adding a new scheduled provisioning profile for the supported Polycom endpoints.

Field	For the endpoint systems being provisioned...	HDX Series	VVVSX Series	FX/EX	ViewStation	QDX Series
General Settings > System Settings > System Settings 1						
Maximum Time in Call (minutes)	Specifies the maximum number of minutes allowed for a call. Enter 0 to remove any limit.	Y	Y	Y	Y	Y
Allow Mixed IP and ISDN calls	Specifies whether users can make multipoint calls that include both IP and H.320 sites.	Y	Y	—	—	—
Auto Answer Point-to-Point Calls	Specifies whether to set the endpoint system to answer incoming point-to-point calls automatically.	Y	Y	Y	Y	Y

Field	For the endpoint systems being provisioned...	HDX Series	VV/SX Series	FX/EX	ViewStation	QDX Series
Auto Answer Multipoint Calls	Specifies whether to set the endpoint system to answer incoming multipoint calls automatically.	Y	Y	Y	—	—
Allow Dialing	Allow users to place calls. You can still place calls from the web interface.	—	—	Y	Y	
Allow Directory Changes	Specifies whether users can save changes to the directory or contacts/favorites list.	Y	Y	Y	Y	Y
Confirm Directory Additions Upon Call Disconnect	Specifies whether users are prompted to confirm deletions of directory entries.	Y	Y	—	—	Y
Confirm Directory Deletions	Specifies whether users are prompted to confirm new directory entries when saving the information for the last site called.	Y	Y	—	—	Y
Allow Access to User Setup	Specifies whether the User Settings screen is accessible to users via the System screen. Select this option to allow users to change limited environmental settings.	Y	Y	Y	Y	Y
General Settings > System Settings > System Settings 2						
Far Site Name Display	Specifies how long the far site name to appear on the screen when the call is first connected.	Y	Y	—	—	Y
Display Time in Call	Displays time that the current call has been connected	Y	Y	—	—	Y
Keypad Audio Confirmation	Allows the user to hear a voice confirmation of the numbers selected with the remote control.	Y	Y	Y	Y	Y
Call Detail Report	Collects call data.	Y	Y	—	—	Y
Recent Calls	Provides navigational tool for call history.	Y	Y	—	—	Y
Display IP and ISDN Information	<ul style="list-style-type: none"> Both – Displays both number types on the system's Home screen. IP only – Display the system IP number on the Home screen. ISDN only – Displays the system ISDN number on the Home screen. None – The system will not display contact numbers on the Home screen. 	—	—	Y	Y	
Show Speed Dial	Allow the user to disable the Speed Dial page and go directly to the Address Book.	—	—	Y	Y	
Color Scheme	Enables the customization of the look of the system with five different color schemes.		Y	—	—	

Field	For the endpoint systems being provisioned...	HDX Series	VVSVX Series	FX/EX	ViewStation	QDX Series
Screen Saver Wait Time	The time the system will delay before going into standby mode after nonuse		Y	Y		Y
General Settings > Home Screen Settings > Home Screen Settings 1						
Dialing Display	Dialing entry field - Includes the dialing entry field on the Home screen. Display Marquee - Allows the addition of text to the dialing entry field of the Home screen.	Y	Y	—	—	Y
Enter Marquee Text	Enter the Marquee text that will appear in the “Dialing entry field” when Display Marquee is selected.	Y	Y	—	—	Y
Call Quality	Allow users to select the speed/bandwidth of the call.	Y	Y			Y
Display H.323 Extension	Displays the IP dialing extension on the main call screen	Y	Y			Y
Directory	Includes the Directory button on the Home screen.	Y	Y			Y
System	Includes the System button on the Home screen.	Y	Y			Y
Multipoint	Includes the Multipoint navigational item on the Home screen.	Y	Y			
General Settings > Home Screen Settings > Home Screen Settings 2						
System Name	Enable when the system name is to be displayed on the Home Screen.	Y	Y			Y
IP or ISDN Information	<ul style="list-style-type: none"> Both – Displays both number types on the system's Home screen. IP only – Display the system IP number on the Home screen. ISDN only – Displays the system ISDN number on the Home screen. None – The system will not display contact numbers on the Home screen. 	Y	Y			
Local Date and Time	Displays the local time on the Home screen.	Y	Y			Y
Enable Availability Control	Displays availability icons on the Home screen.	Y	Y			Y
Sites	Displays icons created for frequently called sites on the Home screen.	Y	Y			Y
Last Number Dialed	Displays the last number dialed on the Home screen.	Y	Y			Y

Field	For the endpoint systems being provisioned...	HDX Series	VV/SX Series	FX/EX	ViewStation	QDX Series
General Settings > Security						
Remote Access Password	Specifies the password for administrator access when logging in to the system remotely. When the remote access password is set, users must enter it to manage the system from a computer. The remote access password must not contain spaces.	Y	Y	Y	Y	Y
Meeting Password	Specifies the password users must supply to join multipoint calls on this system if the call uses the internal multipoint option, rather than a bridge. The meeting password must not contain spaces. Do not set a meeting password if multipoint calls will include audio-only endpoints. Audio-only endpoints cannot participate in password-protected calls.	Y	Y	Y	Y	
Software Update Password	Specifies the password users must enter to update the software on their endpoint system.			Y	Y	
Enable FTP Access	Specifies that the endpoint system can be accessed via an FTP session. Note: The system restarts if you change the remote access settings. This setting does not deactivate the associated port, only the application. Use Web Access Port to disable the port.		Y	Y	Y	
Enable Web Access	Specifies that the endpoint system can be accessed via its web interface. Note: The system restarts if you change the remote access settings. This setting does not deactivate the associated port, only the application. Use Web Access Port to disable the port.	Y	Y	Y	Y	Y
Enable Telnet Access	Specifies that the endpoint system can be accessed via a telnet session. Note: The system restarts if you change the remote access settings. This setting does not deactivate the associated port, only the application. Use Web Access Port to disable the port.	Y	Y	Y	Y	Y

Field	For the endpoint systems being provisioned...	HDX Series	VV/SX Series	FX/EX	ViewStation	QDX Series
AES Encryption	Specifies how to encrypt calls with other sites that support AES encryption. <ul style="list-style-type: none"> Off—AES Encryption is disabled. When Available—AES Encryption is used with any endpoint that supports it, even if the other endpoints in the call don't support it. Required for Video Calls Only—AES Encryption is used for all video endpoints in the call. Analog phone and voice over ISDN connections are allowed. Video endpoints must support AES Encryption to participate in the call. Required for All Calls—AES Encryption is used for all video endpoints in the call. Analog phone and voice over ISDN connections are not allowed. All endpoints must support AES Encryption to participate in the call. 	Y	Y			Y
Enable SNMP Access	Specifies that the endpoint system can be accessed via an SNMP monitoring system. Note: The system restarts if you change the remote access settings. This setting does not deactivate the associated port, only the application. Use Web Access Port to disable the port.			Y	Y	
General Settings > Date and Time 1						
Date Format	Specifies the preferred format preference for the date and time display and lets you enter your local date and time.	Y	Y			Y
Time Format		Y	Y			Y
Month		Y	Y			Y
Day		Y	Y			Y
Year		Y	Y			Y
Hour		Y	Y			Y
Minute		Y	Y			Y
AM/PM		Y	Y			Y
Primary Time Server Address						
Auto Adjust for Daylight Saving Time	Specifies the daylight savings time setting. When this setting is enabled, the system clock automatically changes for daylight saving time.	Y	Y		Y	Y
Time Difference from GMT	Specifies the time difference between GMT (Greenwich Mean Time) and the endpoint system's location.	Y	Y		Y	Y

Field	For the endpoint systems being provisioned...	HDX Series	VVSV Series	FX/EX	ViewStation	QDX Series
Time Server	Specifies connection to a time server for automatic system time settings.	Y	Y			Y
Primary Time Server Address	Specifies the address of the time server to use when Time Server is set to Manual.	Y	Y			Y
Video Network > IP Network > Call Preferences						
Enable IP H.323	Allows the system to make IP calls	Y	Y	—		Y
Enable H.239	Specifies standards-based People+Content data collaboration. Enable this option if you know that H.239 is supported by the far sites you will call. If callers experience issues when sharing content with other Polycom systems, disable this setting.	Y	Y	—		Y
Enable Transcoding	Specifies whether the system allows each far-site system to connect at the best possible call rate and audio/video algorithm. If transcoding is disabled, the Polycom HDX system down-speeds all connections to the same call rate.	Y	Y	—		
ISDN Gateway	Allows users to place IP-to-ISDN calls through a gateway.	Y	Y	—		Y
IP Gateway	Allows users to place ISDN-to-IP or IP-to-IP calls through a gateway.	Y	—	—		
Video Network > IP Network > Gatekeeper						
Use Gatekeeper	Specifies whether to use a gatekeeper. Gateways and gatekeepers are required for calls between IP and ISDN. <ul style="list-style-type: none"> Off — Calls do not use a gatekeeper. Auto — System attempts to automatically find an available gatekeeper. Specify — Calls use the specified gatekeeper. Enter the gatekeeper's IP address or name (for example, gatekeeper.companyname.usa.com, or 10.11.12.13). 	Y	Y	Y	Y	Y
Gatekeeper IP Address	If you chose to use an automatically selected gatekeeper, this area displays the gatekeeper's IP address. If you chose to specify a gatekeeper, enter the IP address.	Y	Y	Y	Y	Y
Outbound Call Route	Choices: <ul style="list-style-type: none"> Gateway ISDN 	—	—	Y	Y	

Field	For the endpoint systems being provisioned...	HDX Series	VV/SX Series	FX/EX	ViewStation	QDX Series
Use Gatekeeper for Multipoint Calls	Specify whether multipoint calls use the system's internal multipoint capability or the Conference on Demand feature.	Y	Y	Y		
Send Preferred Alias Only to Gatekeeper		—	—	Y		
Video Network > IP Network > Gateway Number						
Country Code	Specifies the country code for the system's location	Y	Y	—		
Area Code	Specifies the area or city code for the system's location	Y	Y	—		
Gateway Number	Specifies the gateway's number	Y	Y	—		
Gateway Number Type	<p>Specifies the number type users enter to call this system:</p> <ul style="list-style-type: none"> Direct Inward Dial — Users enter an internal extension to call this system directly. <p>Note</p> <p>If you choose this setting, you must also register the number with the gatekeeper as an E.164 alias.</p> <ul style="list-style-type: none"> Number + Extension — Users enter the gateway number and the system's extension to call this system. 	Y	Y	Y	Y	
Number of digits in DID Number	<p>Specifies the number of digits in the DID number.</p> <p>The national or regional dialing plan for your location determines the standard number of digits. For instance, the US standard is 7 digits.</p>	Y	Y	Y	Y	
Number of digits in Extension	<p>Specifies the number of digits in the extension used when Direct Inward Dial is selected.</p> <p>Your organization's dial plan determines this number.</p>	Y	Y	Y	Y	
Video Network > IP Network > Quality of Service Settings						
Type of Service Field	<p>Specifies the service type and the priority of IP packets sent to the system for video, audio, and far-end camera control:</p> <ul style="list-style-type: none"> IP Precedence — Represents the priority of IP packets sent to the system. The value can be between 0 and 7. DiffServ — Represents a priority level between 0 and 63. If this setting is selected, enter the value in the Type of Service Value field. 	Y	Y	Y	Y	Y

Field	For the endpoint systems being provisioned...	HDX Series	VV/SX Series	FX/EX	ViewStation	QDX Series
Video Type of Service Value	Specifies the IP Precedence or Diffserv value for video packets. This value does not apply to the CMA Desktop system. Its value is set by the client's operating system.	Y	Y	Y		Y
Audio Type of Service Value	Specifies the IP Precedence or Diffserv value for audio packets.	Y	Y	Y		Y
FECC Type of Service Value	Specifies the IP Precedence or Diffserv value for Far End Camera Control packets.	Y	Y	Y		Y
Enable Dynamic Bandwidth	Specifies whether to let the system automatically find the optimum line speed for a call	Y	Y	Y		
Enable PVEC	Allows the system to use PVEC (Polycom Video ErrorConcealment) if packet loss occurs.	Y	Y	Y		Y
Video Network > IP Network > Firewall Settings						
Use Fixed Ports	<p>Specifies whether to define the TCP and UDP ports.</p> <ul style="list-style-type: none"> If the firewall is H.323 compatible or the endpoint systems are not behind a firewall, disable this setting. If the firewall is not H.323 compatible, enable this setting. The endpoint systems will assign a range of ports starting with the TCP and UDP ports you specify. The endpoint system defaults to a range beginning with port 3230 for both TCP and UDP. <p>Note</p> <p>You must open the corresponding ports in the firewall. You must also open the firewall's TCP port 1720 to allow H.323 traffic.</p>	Y	Y	Y	Y	Y
Start TCP Port	<p>Allows you to specify the beginning value for the range of TCP ports used by the endpoint systems. The endpoint systems will automatically assign a range of ports starting with the port you specify.</p> <p>Note</p> <p>You must also open the firewall's TCP port 1720 to allow H.323 traffic.</p>	Y	Y	Y	Y	Y
Start UDP Port	Allows you to specify the beginning value for the range of TCP ports used by the endpoint systems. The endpoint systems will automatically assign a range of ports starting with the port you specify.	Y	Y	Y	Y	Y
System is Behind a NAT	Specifies whether the endpoint systems are behind a NAT firewall.	—	—	Y	Y	

Field	For the endpoint systems being provisioned...	HDX Series	VV/SX Series	FX/EX	ViewStation	QDX Series
NAT Configuration	Specifies whether the endpoint systems should determine the NAT Public WAN Address automatically. <ul style="list-style-type: none"> If the endpoint systems are behind a NAT that allows HTTP traffic, select Auto. If the endpoint systems are behind a NAT that does not allow HTTP traffic, select Manual. Then specify a NAT Public (WAN) Address. If the endpoint systems are not behind a NAT or are connected to the IP network through a virtual private network (VPN), select Off. 	Y	Y			Y
NAT Public (WAN) Address	When NAT Configuration is set to Manual , specifies the address that callers from outside the LAN should use to call the endpoint systems.	Y	Y			Y
NAT is H.323 Compatible	Specifies that the endpoint systems are behind a NAT that is capable of translating H.323 traffic.	Y	Y	Y		Y
Auto Discover NAT Address	Specifies whether to allow the system to automatically discover the NAT firewall address through the domain name server.	—	—	Y	Y	
Address Displayed in Global Directory	Specifies whether or not to include the endpoint system's information in the global directory	Y	Y	—		Y
Video Network > ISDN BRI Protocol						
Enable ISDN H.320	Allows this system to make H.320 (ISDN) calls.	Y	Y	—		
Number of ISDN Channels to Dial in Parallel	Specifies how many channels to dial at one time. You can specify up to eight channels. If you experience network problems, decrease the number. Set this value to 1 for serial dialing. Serial dialing is not recommended unless you have trouble connecting calls using parallel dialing.	Y	Y	—		
ISDN Switch Protocols	Specifies the protocol used by your network's switch.	Y	Y	—		
Outside Line Dialing Prefix	Specifies the ISDN dialing prefix used to call outside the network.	Y	Y	—		

Field	For the endpoint systems being provisioned...	HDX Series	VV/SX Series	FX/EX	ViewStation	QDX Series
Video Network > Preferred Speeds						
Preferred Speed for Placing Calls (Kbps)	Determines the speeds that will be used for IP, ISDN, or International ISDN calls from this endpoint system when: <ul style="list-style-type: none">The Call Quality selection is either unavailable or set to Auto on the Place a Call screenThe call is placed from the directory If the far-site endpoint system does not support the selected speed, the endpoint system automatically negotiates a lower speed.	Y	Y	—		Y
IP Calls		Y	Y	—		Y
ISDN Video Call (H.320)		Y	Y	—		
International ISDN calls		Y	Y	—		
Maximum Speed for Receiving Calls (Kbps)	Allows you to restrict the bandwidth used when receiving IP or ISDN calls. If the far site attempts to call the system at a higher speed than selected here, the call is re-negotiated at the speed specified in this field.	Y	Y	—		Y
IP Calls		Y	Y	—		Y
ISDN Video Call (H.320)		Y	Y	—		
Monitors > Monitors 1						
Number of Monitors						Y
Monitor 1 Options						
Monitor 1	Specifies the monitor's aspect ratio. <ul style="list-style-type: none">4:3 — Select if you are using a regular TV monitor.			—		Y
Video Format	Specifies the monitor's format: <ul style="list-style-type: none">DVI — Select if the monitor is connected to the DVI connector using a DVI or HDMI cable.VGA — Select if the monitor is connected to the DVI connector using a VGA cable.Component YPbPr — Select if the monitor is connected to the DVI connector using component cables. Polycom HDX 8000 series and Polycom HDX 7000 series systems do not support 720p Component format for 50 Hz monitors.S-Video (Polycom HDX 9000 series only) — Select if the monitor is connected to the BNC connectors using an S-Video cable.Composite (Polycom HDX 9000 series only) — Select if the monitor is connected to the BNC connectors using a composite video cable.	Y	Y	—		
Display Icons in Call	Specifies whether to display all on-screen graphics, including icons and help text, during calls.	Y	Y	—		Y

Field	For the endpoint systems being provisioned...	HDX Series	VV/SX Series	FX/EX	ViewStation	QDX Series
Snapshot Timeout	Lets you choose whether to have slides and snapshots time out after a period of four minutes.	—	Y	—		
Dual Monitor Emulation	Specifies whether the system can show multiple views on a single display.	Y	Y	—		
Output Upon Screen Saver Activation	<p>Specifies whether black video or no signal is sent to the monitor when the system goes to sleep and the screen saver activates.</p> <ul style="list-style-type: none"> Select Black to display black video. This is the recommended setting to prevent burn-in for TV monitors. Select No Signal to have the display react as if it is not connected when the system goes to sleep. This is the recommended setting for VGA monitors and projectors. 	Y		—		Y
VGA Resolution		—	Y	—		
Monitor 2 Options	Applies to:	Y	—	—		Y
Monitor 2	<p>Specifies the second monitor's aspect ratio:</p> <ul style="list-style-type: none"> Off — Select if you do not have a second monitor. 4:3 — Select if you are using a regular TV monitor as the second monitor. 	Y	—	—		Y
Video Format	<p>Specifies the monitor's format:</p> <ul style="list-style-type: none"> DVI — Select if the monitor is connected to the DVI connector using a DVI or HDMI cable. VGA — Select if the monitor is connected to the DVI connector using a VGA cable. Component YPbPr — Select if the monitor is connected to the DVI connector using component cables. Polycom HDX 8000 series and Polycom HDX 7000 series systems do not support 720p Component format for 50 Hz monitors. S-Video (Polycom HDX 9000 series only) — Select if the monitor is connected to the BNC connectors using an S-Video cable. Composite (Polycom HDX 9000 series only) — Select if the monitor is connected to the BNC connectors using a composite video cable. 	Y	—	—		Y

Field	For the endpoint systems being provisioned...	HDX Series	VV/SX Series	FX/EX	ViewStation	QDX Series
Output Upon Screen Saver Activation	<p>Specifies whether black video or no signal is sent to the monitor when the system goes to sleep and the screen saver activates.</p> <ul style="list-style-type: none"> Select Black to display black video. This is the recommended setting to prevent burn-in for TV monitors. Select No Signal to have the display react as if it is not connected when the system goes to sleep. This is the recommended setting for VGA monitors and projectors. 	Y	—	—		Y
People Display Mode						Y
Content Display Mode						Y
Color System						Y
<i>Monitor 3 Options</i>						
Monitor 3	<p>Specifies the aspect ratio for recording.</p> <ul style="list-style-type: none"> Off — Select if you do not have a VCR or DVD player connected to record video conferences. 4:3 — Select to record for playback on a standard monitor. 16:9—Select to record for playback on a wide-screen monitor, if your recording device has this capability. <p>See the endpoint product documentation for more information about these selections.</p>	Y	—	—		
Video Format	<p>Specifies the VCR or DVD player's format:</p> <ul style="list-style-type: none"> S-Video — Select if the VCR or DVD player is connected to a Polycom HDX system using an S-Video cable. Composite — Select if the VCR or DVD player is connected to a Polycom HDX system using a composite video cable and S-Video to RCA adapter. 	Y	—	—		
Output Upon Screen Saver Activation	<p>Specifies whether black video or no signal is sent to the VCR or DVD player when the system goes to sleep and the screen saver activates.</p> <ul style="list-style-type: none"> Select Black to send black video. Select No Signal to have the VCR or DVD player react as if it is not connected when the system goes to sleep. 	Y	—	—		

Field	For the endpoint systems being provisioned...	HDX Series	VV/SX Series	FX/EX	ViewStation	QDX Series
VCR/DVD Record Source	Specifies the video source to be recorded to videotape or DVD.	Y	—	—		
Near	<ul style="list-style-type: none"> If Far is enabled, the recorded video will switch to the current far site speaker. If both Near and Far are enabled, the recorded video will switch between near and far sites depending on the current speaker. If Content is enabled, any content sent during the call is recorded. 	Y	—	—		
Far		Y	—	—		
Content		Y	—	—		
Screen Saver Wait Time	The time the system will delay before going into standby mode after nonuse	Y				
Cameras > Cameras 1						
Camera 1 Name	Specifies a name for camera 1.	Y				
Camera 1 Icon	Specifies an icon for camera 1.	Y				
Camera 2 Name	Specifies a name for camera 2.	Y				
Camera 2 Icon	Specifies an icon for camera 2.	Y				
Cameras > Camera Settings						
Camera 1 Name	Specifies a name for camera 1.	Y	Y			Y
Camera 1 Icon	Specifies an icon for camera 1.	Y	Y			Y
Camera 2 Name	Specifies a name for camera 2.	Y	Y			Y
Camera 2 Icon	Specifies an icon for camera 2.	Y	Y			Y
Camera 3 Name	Specifies a name for camera 3.	Y	Y			Y
Camera 3 Icon	Specifies an icon for camera 3.	Y	Y			Y
Cameras > Video Quality						
Camera 1	Specifies Motion or Sharpness for the video input. The default is Sharpness. <ul style="list-style-type: none"> Motion — This setting is for showing people or other video with motion. Sharpness — The picture will be sharp and clear, but moderate to heavy motion at low call rates can cause some frames to be dropped. Sharpness is available in point-to-point H.263 and H.264 calls only. It is recommended for HD calls between 1 Mbps and 2 Mbps. 	Y	Y			Y
Camera 2		Y	Y			Y
Camera 3		Y	Y			Y

Field	For the endpoint systems being provisioned...	HDX Series	VV/SX Series	FX/EX	ViewStation	QDX Series
Video/Camera > Cameras 1						
<i>Snapshot Camera</i>						
Far Control of Near Camera	Specifies whether the far site can pan, tilt, or zoom the near-site camera. When this option is selected, a user at the far site can control the framing and angle of the camera for the best view of the near site.	Y	Y	Y	Y	Y
Backlight Compensation	Specifies whether the camera should automatically adjust for a bright background. Backlight compensation is best used in situations where the subject appears darker than the background.	Y	Y	Y	Y	Y
Primary Camera	Specifies which camera is the main camera.	Y	Y		Y	Y
Camera Direction	Specifies the direction the camera moves when using the arrow buttons on the remote control.	Y	Y	Y	Y	Y
Video/Camera > Monitor Setup						
Snapshot Timeout	Lets you choose whether to have slides and snapshots time out after a period of four minutes.	—	—	Y	Y	
Audio Settings > Audio Settings 1						
Sound Effects Volume	Sets the volume level of the ring tone and user alert tones.	Y	Y	Y	Y	Y
Incoming Video Call	Specifies the ring tone used for incoming calls.	Y	Y			Y
User Alert Tones	Specifies the tone used for user alerts.	Y	Y			Y
Mute Auto Answer Calls	Specifies whether to mute incoming calls. Incoming calls are muted by default until you press the mute on the microphone or on the remote control.	Y	Y	Y	Y	Y
Input Type Level	Sets the volume level for audio input 1.	Y	Y			
Content Input Level	Specifies the volume level for audio input 4 of a Polycom HDX 9000 series or Polycom HDX 8000 series system. Specifies the volume level for audio input 3 of a Polycom HDX 7000 series system. Specifies the volume level for the PC audio input of a Polycom HDX 6000 series or Polycom HDX 4000 series.	Y	Y			
Line Output Level	Sets the volume level for audio output.	Y	Y			
Audio Settings > Audio Settings 2						

Field	For the endpoint systems being provisioned...	HDX Series	VV/SX Series	FX/EX	ViewStation	QDX Series
Master Audio Volume	Sets the volume level for audio from the far site.	Y	Y			Y
Midrange Speakers	Specifies whether to use the system's built-in midrange speaker. You may prefer to turn off the midrange speaker if you connect the audio output to Monitor 1 or if you connect an external speaker system.	—	Y			
Bass	Sets the volume level for the low frequencies without changing the master audio volume.	Y	Y			
Treble	Sets the volume level for the high frequencies without changing the master audio volume.	Y	Y			
LAN Properties > LAN Properties 1						
Connect to My LAN	Enables connection to the local area network	Y	Y			
IP Address	Specifies how the system obtains an IP address. <ul style="list-style-type: none"> Obtain IP Address Automatically — Select if the system gets an IP address from the DHCP server on the LAN. Enter IP Address Manually — Select if the IP address will not be assigned automatically. 	Y	Y			Y
Use the Following IP Address	If you selected Enter IP Address Manually , enter the IP address here.	Y	Y			Y
LAN Properties > LAN Properties 2						
DNS Servers	Displays the DNS servers currently assigned to the system. If the system does not automatically obtain a DNS server address, enter up to four DNS servers here. Changing this setting causes the system to restart.	Y	Y			Y
Default Gateway	Displays the gateway currently assigned to the system. If the system does not automatically obtain a gateway IP address, enter one here. Changing this setting causes the system to restart.	Y	Y			Y
Subnet Mask	Displays the subnet mask currently assigned to the system. If the system does not automatically obtain a subnet mask, enter one here. Changing this setting causes the system to restart.	Y	Y			Y
WINS Server	Displays the server running the Windows Internet Name Service	—	Y			

Field	For the endpoint systems being provisioned...	HDX Series	VV/SX Series	FX/EX	ViewStation	QDX Series
WINS Resolution	Enables connection to the WINS Server for URL resolution	—	Y			
LAN Speed	<p>Specify the LAN speed to use. Note that the setting you choose must be supported by the switch.</p> <p>Choose Auto to have the network switch negotiate the speed automatically. In this case, the switch must also be set to Auto. Choosing Auto automatically sets Duplex Mode to Auto.</p> <p>If you choose 10 Mbps, 100 Mbps, or 1000 Mbps you must set Duplex Mode to Half or Full.</p> <p>Changing this setting causes the system to restart.</p> <p>Note</p> <p>Mismatches with the network switch settings may lead to unexpected behaviors.</p>	Y	Y			Y
Duplex Mode	<p>Specify the duplex mode to use. Note that the Duplex mode you choose must be supported by the switch.</p> <p>Choose Auto to have the network switch negotiate the Duplex mode automatically. In this case, the switch must also be set to Auto. Choosing Auto automatically sets LAN Speed to Auto.</p> <p>Changing this setting causes the system to restart.</p>	Y	Y			Y
Global Services > Directory Servers						
Global Directory (GDS)	Specifies the IP address or DNS address of the Global Directory Server.	Y	Y	Y	Y	Y
Password	Lets you enter the global directory password, if there is one.	Y	Y	Y	Y	Y
Display Name in Global Directory	Specifies whether to display the system's name in the global directories of other registered systems. Global Address	Y	Y	—		Y
Display Global Addresses	Displays other registered systems in the global directory.	Y	Y	Y	Y	Y
Register	Registers this system with the Global Directory Server.	Y	Y	Y	Y	Y
Save Global Directory to System	Copies the global directory to this local system. When this setting is disabled, the system can display no more than 1,000 global directory entries. When this setting is enabled, the system can display up to 4,000 global directory entries.	Y	Y	—		Y

Field	For the endpoint systems being provisioned...	HDX Series	VVSV Series	FX/EX	ViewStation	QDX Series
LAN/H.323 > Global Directory (GDS) > Preferences						
Show Addresses in Address Book		—	—	Y	Y	
Preferred Speed for Placing Calls (Kbps)	Determines the speeds that will be used for IP, ISDN, or International ISDN calls from this endpoint system when:	—	—	Y	Y	
ISDN Video Call (H.320)	<ul style="list-style-type: none">The Call Quality selection is either unavailable or set to Auto on the Place a Call screenThe call is placed from the directory	—	—	Y	Y	
International ISDN calls	If the far-site endpoint system does not support the selected speed, the endpoint system automatically negotiates a lower speed.	—	—	Y	Y	
IP Calls		—	—	Y	Y	
LAN/H.323 > Global Directory (GDS) > Preferred Alias						
Preferred Alias	Possible values include: <ul style="list-style-type: none">Gateway NumberISDN NumberCalled Party Line IdentifierExtension	—	—	Y	Y	
Global Services > Dialing Rules 1						
Number of digits in Extension	Specifies the number of digits in the extension. Your organization's dial plan determines this number.	—	—	Y	Y	
International Dialing Prefix	Specifies the dialing prefix needed for international calls	Y	Y	Y	Y	
Public Network Access	Specifies if calls can be made to the public network	—	—	Y	Y	
Public Network Dialing Prefix	Specifies the dialing prefix used to call out to endpoints on the public network when the endpoint is not in the same area code as the system	—	—	Y	Y	
Public Network (same area code) Prefix	Specifies the dialing prefix used to call out to endpoints on the public network when the endpoint is in the same area code as the system	—	—	Y	Y	
Private Network Access	Specifies if calls can be made to the private network	—	—	Y	Y	
Private Network Dialing Prefix	Specifies the dialing prefix used to call outside the network	—	—	Y	Y	
Always Dial Area Code	Specify whether the phone number must always include an area code	Y	Y	—		

Field	For the endpoint systems being provisioned...	HDX Series	VV/SX Series	FX/EX	ViewStation	QDX Series
Dial 1+ for all USA Calls	Specify whether to preface calls within the United States with 1	Y	Y	—		
Global Services > Dialing Rules 2						
If Area Code Equals/ Dial Prefix Pairs	Create additional dialing rules and routing based on area code	—	—	Y	Y	
Global Services > Account Validation						
Require Account Number to Dial	Specify whether to require an account number for placing calls and whether that number should be validated by the system.	Y	Y		Y	
Validate Account Number	Specify whether to require an account number for placing calls and whether that number should be validated by the system.	Y	Y		Y	
Global Services > My Information						
Contact Person	Specifies the name of the person responsible for this system	Y	Y		Y	Y
Contact Number	Specifies the phone number of the person responsible for this system	Y	Y		Y	Y
Contact Email	Specifies the email address of the person responsible for this system	Y	Y		Y	Y
Contact Fax	Specifies the Fax number of the person responsible for this system	Y	Y		Y	Y
Tech Support	Specifies the contact information for Technical Support for this system	Y	Y			Y
City	Specifies the location of the person responsible for this system	Y	Y		Y	Y
State/Province		Y	Y		Y	Y
Country		Y	Y		Y	Y
Video Network > IP Network > Gateway Setup						
Speed	Enter a prefix or suffix for each bandwidth allowed for gateway calls. Associating prefixes and suffixes with particular bandwidths on your gateway can optimize the use of bandwidth by your organization. Be sure the gateway is configured to use the same prefixes and suffixes you define for the system.	Y	Y	Y	Y	
Prefix		Y	Y	Y	Y	
Suffix		Y	Y	Y	Y	

Scheduled Provisioning Notes

Some notes about scheduled provisioning profiles and the scheduled provisioning of endpoints:

- Each page in the scheduled **Provisioning Fields** dialog box has a **Provision This Page** option. When this option is selected, the system provisions all of the values on that page. When this option is not selected, the system does not provision any of the values on that page. At least one page must be provisioned, or the system returns an error stating, “No data to save in profile. Either press **Cancel** or add pages.”
- Until the CMA system successfully provisions an endpoint scheduled for provisioning, provisioning remains in the **Pending** state and the system attempts to provision the endpoint until it succeeds or until the provisioning is cancelled.
- If an endpoint scheduled for provisioning is **In a Call**, the system waits until the call ends before provisioning the endpoint. The system checks the endpoint at 15 minute intervals.
- If an endpoint scheduled for provisioning is **Offline**, the system attempts to connect to it at 60 minute intervals until the endpoint is **Online**.
- Provisioning may reboot the endpoint
- You can schedule provisioning for an unlimited number of endpoints, but the system may limit the number of active provisioning processes

Endpoint Gatekeeper Registration Policies

If the CMA system gatekeeper registration policy allows endpoints to register automatically (that is, a primary gatekeeper setting of **Allow Registration of All Endpoints**, **Allow Registration of Endpoints in Defined Sites**, or **Allow Registration of Endpoints with Defined E.164 Prefixes**), those registered endpoints are automatically added to the endpoint list.

If the CMA gatekeeper registration policy does not allow endpoints to register automatically (that is, a gatekeeper setting of **Allow Registration of Predefined Endpoints Only**), you must manually add all endpoints to the CMA system.

No matter what the gatekeeper registration policy, any endpoint that is automatically provisioned, any endpoint that is registered with the Global Address Book, and any endpoint that is added manually to the CMA system can automatically register with the gatekeeper. For more information, see [“Device Registration”](#) on page 396.



Note

You can manually add endpoints to the CMA system for monitoring purposes only.

Endpoint Software Updates

The CMA system software update feature, which requires a software update profile for the endpoint type and model, allows an administrator to upgrade the software on one or more endpoints with a standard software package. This eliminates the need to upgrade each endpoint individually.

The CMA system supports two exclusive software update processes: automatic and scheduled. Automatic and scheduled software update are exclusive endpoint management scenarios. Endpoints enabled for automatic software update should not be scheduled for software updates through the system.



Note

Polycom recommends that all endpoints in a region (that is, a gatekeeper zone) be managed by a single management system.

For more information, see:

- [Automatic Software Updates](#)
- [Scheduled Software Updates](#)

Automatic Software Updates

Automatic software update, which controls the endpoint's software version level, is tied to the endpoint type. Currently, the automatic software update feature is only available for these endpoint types.

- Polycom HDX system endpoints deployed in dynamic management mode
- Polycom RealPresence Group Series
- Polycom CMA Desktop systems

How Automatic Software Update Works

In dynamic management mode, when a endpoint starts up and at designated intervals thereafter, it automatically polls the CMA system for a newer software update package. If a software update is necessary, the package is sent in XML format over a secure HTTPS connection.

Endpoints do not poll for software update packages if they are in a call. They restart polling after the call ends.

Automatic Software Update Profiles

Automatic software update is enabled at the endpoint, but the CMA system must have an automatic software update profile for the endpoint type to fulfill the process. A default automatic software update profile — with the

description **CMA Desktop - shipped version**—is available for the Polycom CMA Desktop client. Default automatic software update profiles are not available for other endpoint systems. To create an automatic software update profile, you upload the software package and create a profile for the update.

Automatic Software Update Versions

After creating an automatic software update profile, you can use the **Version to use** and **Allow this version or newer** selections to manage the roll out of software update packages. These selections also allow you to manage the release of multiple software packages for the same endpoint type.

Here's how it works: All endpoints have a current version of software. To automatically overwrite that current software with a different software version on all dynamically managed endpoint systems:

- 1 You first create a new automatic software update profile that includes the new software update package.
- 2 Then to activate the roll out, you change the **Version to use** selection from the current value (**None** by default) to the new version number and **Update** the page.

The next time a dynamically managed endpoint polls the CMA system, it will detect that it has a different software version than the **Version to use** selection, so it will automatically download and install the identified software update package. Use this method to force users to use a specific software version.



Note

Until the **Version to use** selection is enabled, the automatic software update is not activated.

If you also enable the **Allow this version or newer** selection, anytime you package a newer version of software into an automatic software profile that package will be automatically installed on all dynamically managed endpoint systems.

Some important things to note about software versions

- Newer software is identified by the version number. If the **Allow this version or newer** selection is enabled, when a dynamically managed endpoint polls the CMA system, the system will compare the current software version number with the packaged software version numbers. The CMA system will send the software package with the highest version number to the endpoint.
- You can also use the **Version to use** selection to roll endpoints back to older software versions. If you change the **Version to use** selection to an older software version and clear the **Allow this version or newer** selection, the CMA system will send the specifically identified software package to the endpoint even if it is an older version.



Note

Currently to roll back a Polycom CMA Desktop client to an older version, you must first remove the existing Polycom CMA Desktop client via the Windows **Add or Remove Software** selection. Then you can install the older software package.

Peripheral Software Updates

You can update the platform (operating system) and applications (if applicable) for peripherals connected to endpoints. Peripheral software updates can be in any of the following states:

- **Production** - The software update is configured for one or more groups that are using the software in production.
- **Trial** - The software update is configured for one or more groups that are trialing the software.
- **Both** - The software update is configured for one or more groups that are trialing the software and for one or groups are using the software in production.



Note

When doing peripheral upgrades on redundant systems running Microsoft SQL Server 2005 or 2008 R1, you may receive an SQL server exception. To resolve this exception, upload the peripheral upgrade package to the secondary server as well.

Scheduled Software Updates

The scheduled software update feature is enabled at the CMA system. An administrator with **System Setup** permissions can schedule software updates for one endpoint or a group of endpoints to occur immediately or for a date and time in the future.

Scheduled software updates are available for these endpoint types.

- ViewStation
- ViewStation FX & EX
- V and VSX Series
- TANDBERG MXP series
- HDX Series--Polycom HDX systems operating in standard management mode

Some notes about scheduled software updates:

- Until the CMA system successfully updates an endpoint scheduled for updating, the update remains in the **Pending** or **In Progress** state and the CMA system attempts to update the endpoint until it succeeds or until the update is cancelled.

- If an endpoint scheduled for update is **In a Call**, the CMA system waits until the call ends before updating the endpoint. The system checks the endpoint at 15 minute intervals.
- If an endpoint scheduled for update is **Offline**, the CMA system attempts to connect to the endpoint every hour until the endpoint is **Online**.
- A software update may reboot the endpoint.

Endpoint Passwords

A CMA system can manage Polycom endpoints only when the password in the device record matches the password in the endpoint. Matching passwords are required to:

- Schedule provisioning of an endpoint through a CMA system.
- Use the Scheduled Software Update feature.
- Monitor the endpoint from the **Endpoint > Monitor View**.

You can update the password for certain endpoint systems through scheduled provisioning only after you have entered the matching password in the CMA system. In this case, you must instruct end-users not to change the password.



Note

Some companies select an administrative password that is used for all endpoints and regularly updated through provisioning.

For third-party endpoints, passwords may be required to access the endpoint management software.

For information about restrictions in changing passwords for a specific endpoint, see the documentation for the endpoint.

Considerations for Third-Party Endpoints

The CMA system includes additional command and control for select TANDBERG C Series, TANDBERG Edge, and LifeSize Team and Express endpoints. The CMA system can send a Reboot command to these endpoints, and the endpoints can receive and act on the command. In addition, the CMA system can:

- Discover these endpoints by searching for them within a range of IP addresses.
- Complete the initial configuration of these endpoints.
- Schedule and launch point-to-point conferences on these endpoints.

- Launch the management interface for these endpoints.

In the following sections, some additional considerations for supporting third-party endpoints are discussed, including

- [Enable TANDBERG Endpoints Global Address Book Access](#)
- [Enabling Management of LifeSize Endpoints](#)
- [Monitoring](#)
- [Scheduled Provisioning of Selected TANDBERG Endpoints](#)
- [Scheduled Provisioning of LifeSize Endpoints](#)
- [Reporting](#)

Enable TANDBERG Endpoints Global Address Book Access

With CMA system, users of the TANDBERG 150, 990, 880, 770 MXP, TANDBERG C Series, and TANDBERG Edge can access the Polycom Global Address Book, so they can see the endpoints in the Global Address Book. (Note that any third-party endpoint that is registered to the CMA system gatekeeper is displayed in the Global Address Book.)

The timing of the endpoint's connection with the Global Address Book can affect the success of its connection. We recommend the following process:

- 1 At the endpoint, enter the information required for directory set up including the Polycom Global Address Book/CMA system IP address and the path. To do this, on the endpoint, go to **Endpoint Configuration > General > External Phone Book Settings**.
- 2 Wait for the connections to take effect.
- 3 At the CMA system, go to **Endpoint > Monitor View** and verify the endpoint's Global Address Book connection status is green.

Considerations for LifeSize Endpoints

Consider the following when you must support LifeSize endpoints:

- [“Enabling Management of LifeSize Endpoints”](#) on page 137
- [“Provisioning of LifeSize Passwords”](#) on page 164
- [“Scheduled Provisioning of LifeSize Endpoints”](#) on page 157

Enabling Management of LifeSize Endpoints

To facilitate management of LifeSize endpoints, a CMA system administrator must enable the **Default Passwords for LifeSize Endpoint Management** option and enter the SSH and web UI passwords for the LifeSize endpoints.

To enable LifeSize endpoint management

- 1** On the CMA system, go to **Admin > Management and Security > Endpoint Management Settings**.
- 2** In the **Default Passwords for LifeSize Endpoint Management** section of the **Endpoint Management Settings** page, enable **Use Default Passwords**.
- 3** Enter the **Password for SSH User** and confirm the password. Refer to the LifeSize system documentation for information on using SSH to connect to the endpoint, then enter the same SSH password here.
- 4** Enter the **Password for Web UI User** and confirm the password. Refer to the LifeSize system documentation for information on using a web browser to connect to the endpoint, then enter the same web UI password here.
- 5** Click **Update**.

**Note**

For the CMA system to successfully manage a LifeSize endpoint, SSH must be enabled on the endpoint. SSH can be enabled on the endpoint through device provisioning.

Monitoring

The CMA system can monitor select TANDBERG C Series, TANDBERG Edge, and LifeSize Team and Express endpoints, so when properly configured, the CMA system can provide online/offline status and alerts, display call status, and provide image support including near and far end images for these endpoints.

Scheduled Provisioning of Selected TANDBERG Endpoints

The following table identifies the fields that the CMA system can provision for TANDBERG 150, 990, 880, 770 MXP, and TANDBERG C Series endpoints.

See the appropriate TANDBERG product documentation for more information about these fields and their acceptable values. See [“Scheduled Provisioning Operations”](#) on page 186 for information on implementing scheduled provisioning of endpoints.

Field Name	Provisioned for supported Tandberg models?		
	MXP Models 990/880/770	MXP Model T150	C Series
AdditionalCamera Type	Y	N	N
AlertSpeaker Mode	Y	Y	N
AlertTone Telephony	Y	Y	N
AlertTone VideoTelephony	Y	Y	N
AlertTone Volume	Y	Y	N
AllowLatency	Y	N	N
Audio AGC	N	Y	N
Audio AGC AUX	Y	N	N
Audio AGC Microphones	Y	N	N
Audio AGC Received	Y	N	N
Audio AGC VCR	Y	N	N
Audio AudioModule	Y	N	N
Audio AutoMute	Y	Y	N
Audio Delay AUX	Y	N	N
Audio Delay VCR	Y	N	N
Audio EchoControl	N	Y	N
Audio EchoControl 1 through 4	Y	N	N
Audio Feedback Mode	Y	N	N
Audio Inputs Line 1 through 3	Y	N	Y
Level	Y	N	Y
Mode	Y	N	N
Audio Inputs Microphone 1 through 3	Y	N	N
Level	Y	N	N
Mode	Y	N	Y
Audio KeyTones	Y	Y	Y
Audio LocalDetection Mode	Y	N	Y
Audio Loudspeaker	N	Y	Y

Field Name	Provisioned for supported Tandberg models?		
	MXP Models 990/880/770	MXP Model T150	C Series
Audio MicrophoneMixer Mode	Y	N	N
Audio Microphones Mode	Y	N	N
Audio Outputs Line 1 through 3	Y	N	N
Level	Y	N	N
Mode	Y	N	Y
Type	Y	N	Y
Audio Stereo	Y	N	Y
Audio StereoSpeakers	Y	N	Y
Audio VCRRDucking	Y	N	Y
Audio Volume	Y	Y	Y
AutoAnswer Delay	Y	Y	N
AutoAnswer Device	N	Y	N
AutoAnswer Mode	Y	Y	N
AutoLayout Mode	Y	N	N
AutoPIP Mode	Y	N	N
AutoPIP TimeOut	Y	N	Y
Bonding Rebonding	Y	N	Y
Bonding Timer	Y	N	N
CallManager Address	Y	Y	N
CallVideoSource	Y	N	N
Cameras 1 through 13	Y	N	Y
Backlight	Y	N	Y
Brightness Level	Y	N	Y
Brightness Mode	Y	N	Y
DualVisca	Y	N	Y
Focus Mode	Y	N	Y
Gamma Level	Y	N	Y
Gamma Mode	Y	N	Y

Field Name	Provisioned for supported Tandberg models?		
	MXP Models 990/880/770	MXP Model T150	C Series
IR	Y	N	N
Mirror	Y	N	N
Whitebalance Level	Y	N	N
Whitebalance Mode	Y	N	Y
CameraDVI Mode	Y	N	N
CameraSleep Mode	Y	N	N
CameraSwUpgrade	Y	N	N
CameraTracking Speed	Y	N	N
Conference AAC-LD	Y	N	N
Conference AAC-LD-128-Mono	Y	N	N
Conference AAC-LD-128-Threshold	Y	N	N
Conference AIM	Y	Y	N
Conference AllowIncomingCallInCall	Y	N	N
Conference AllowIncomingMSCall	Y	N	N
Conference AllowIncomingTlphCall	Y	N	Y
Conference BillingCode	Y	Y	Y
Conference DefaultCall CallRate	Y	Y	Y
Conference DefaultCall NetProfile	Y	Y	Y
Conference DefaultCall Restrict	Y	Y	Y
Conference Downspeed	Y	N	Y
Conference Encryption Mode	Y	Y	Y
Conference Encryption Type	Y	N	Y
Conference FallbackToTelephony	Y	Y	Y
Conference FarTlphEchoSupression	Y	N	Y
Conference FloorToFull	Y	N	Y
Conference G722	Y	Y	Y
Conference G722.1	Y	Y	N
Conference G728	Y	N	N

Field Name	Provisioned for supported Tandberg models?		
	MXP Models 990/880/770	MXP Model T150	C Series
Conference H239	Y	Y	N
Conference H263	Y	Y	N
Conference H264	Y	Y	N
Conference H264RCDO	Y	N	N
Conference H331	Y	N	N
Conference IPDualstreamRate	Y	N	N
Conference IPLR Transmit	Y	Y	N
Conference MailBox URI	N	Y	N
Conference MaxCallLength	Y	Y	N
Conference NaturalVideo	Y	N	N
Conference PeriodicIntra	Y	N	N
Conference PictureMode	Y	N	N
Conference SIP URI	N	Y	N
Conference VideoQualityCP	Y	N	N
Conference VideoText	Y	N	N
Conference VideoTextTimeout	Y	N	N
Conference WebSnapshots	Y	N	N
CorporateDirectory Address	Y	Y	N
CorporateDirectory Mode	Y	Y	N
CorporateDirectory Path	Y	Y	N
CorporateDirectory Protocol	Y	N	N
DefaultPIPPosition	Y	N	Y
Directory CallLog	Y	Y	Y
Directory SmartSearch	Y	Y	Y
DoNotDisturb Mode	Y	N	N
DualMonitor Mode	Y	N	Y
DuoVideoSource	Y	N	Y
DynamicResolution Mode	Y	N	N

Field Name	Provisioned for supported Tandberg models?		
	MXP Models 990/880/770	MXP Model T150	C Series
E1 Interface CRC4	Y	N	N
Ethernet 1 Speed	Y	Y	Y
Ethernet 2 Speed	Y	Y	N
ExternalNetwork Callcontrol	Y	N	Y
ExternalNetwork Clocking	Y	N	N
ExternalNetwork DTRPulse	Y	N	N
ExternalServices Address	Y	N	Y
ExternalServices Mode	Y	N	N
ExternalServices Path	Y	N	N
ExternalServices Protocol	Y	N	N
FECC Mode	Y	N	N
FeedbackFilter Call	Y	N	N
FeedbackFilter Conference	Y	N	N
FTP Mode	Y	Y	N
G703 Callcontrol	Y	N	N
G703 Interface MaxChannels	Y	N	N
G703 Interface StartChannel	Y	N	N
G703 Linecoding	Y	N	Y
G703 PhysicalLayer	Y	N	N
H320 NetType	Y	N	N
H323 Mode	Y	Y	N
H323CallSetup Mode	Y	Y	N
H323Gatekeeper Address	Y	Y	N
H323Gatekeeper Authentication ID	Y	Y	N
H323Gatekeeper Authentication Mode	Y	Y	N
H323Gatekeeper Authentication Password	Y	Y	N
H323Gatekeeper Avaya AnnexH	Y	Y	N

Field Name	Provisioned for supported Tandberg models?		
	MXP Models 990/880/770	MXP Model T150	C Series
H323Gatekeeper Avaya Mode	Y	Y	N
H323Gatekeeper Avaya MultipointCount	Y	Y	N
H323Gatekeeper Avaya Password	Y	Y	N
H323Gatekeeper Discovery	Y	Y	N
H323Gatekeeper MultipleAlias	Y	Y	N
H323Prefix	Y	N	N
HTTP Mode	Y	Y	N
HTTPS Mode	Y	Y	N
HTTPS VerifyServerCertificate	Y	N	N
IdReport H323	Y	Y	N
IEEE802.1x AnonymousIdentity	Y	Y	N
IEEE802.1x EAP-MD5	Y	N	N
IEEE802.1x EAP-PEAP	Y	Y	N
IEEE802.1x EAP-TTLS	Y	Y	N
IEEE802.1x Identity	N	Y	N
IEEE802.1x Mode	Y	N	N
IEEE802.1x Password	Y	Y	N
IMUX Custom bw1152 Prefix	Y	N	N
IMUX Custom bw1152 Suffix	Y	N	N
IMUX Custom bw1152R Prefix	Y	N	N
IMUX Custom bw1152R Suffix	Y	N	N
IMUX Custom bw128 Prefix	Y	N	N
IMUX Custom bw128 Suffix	Y	N	N
IMUX Custom bw128R Prefix	Y	N	N
IMUX Custom bw128R Suffix	Y	N	N
IMUX Custom bw1472 Prefix	Y	N	N
IMUX Custom bw1472 Suffix	Y	N	N

Field Name	Provisioned for supported Tandberg models?		
	MXP Models 990/880/770	MXP Model T150	C Series
IMUX Custom bw1472R Prefix	Y	N	N
IMUX Custom bw1472R Suffix	Y	N	N
IMUX Custom bw192 Prefix	Y	N	N
IMUX Custom bw192 Suffix	Y	N	N
IMUX Custom bw1920 Prefix	Y	N	N
IMUX Custom bw1920 Suffix	Y	N	N
IMUX Custom bw1920R Prefix	Y	N	N
IMUX Custom bw1920R Suffix	Y	N	N
IMUX Custom bw192R Prefix	Y	N	N
IMUX Custom bw192R Suffix	Y	N	N
IMUX Custom bw256 Prefix	Y	N	N
IMUX Custom bw256 Suffix	Y	N	N
IMUX Custom bw256R Prefix	Y	N	N
IMUX Custom bw256R Suffix	Y	N	N
IMUX Custom bw320 Prefix	Y	N	N
IMUX Custom bw320 Suffix	Y	N	N
IMUX Custom bw320R Prefix	Y	N	N
IMUX Custom bw320R Suffix	Y	N	N
IMUX Custom bw384 Prefix	Y	N	N
IMUX Custom bw384 Suffix	Y	N	N
IMUX Custom bw384R Prefix	Y	N	Y
IMUX Custom bw384R Suffix	Y	N	Y
IMUX Custom bw512 Prefix	Y	N	Y
IMUX Custom bw512 Suffix	Y	N	Y
IMUX Custom bw512R Prefix	Y	N	Y
IMUX Custom bw512R Suffix	Y	N	Y
IMUX Custom bw64 Prefix	Y	N	Y
IMUX Custom bw64 Suffix	Y	N	Y

Field Name	Provisioned for supported Tandberg models?		
	MXP Models 990/880/770	MXP Model T150	C Series
IMUX Custom bw64R Prefix	Y	N	Y
IMUX Custom bw64R Suffix	Y	N	N
IMUX Custom bw768 Prefix	Y	N	N
IMUX Custom bw768 Suffix	Y	N	N
IMUX Custom bw768R Prefix	Y	N	N
IMUX Custom bw768R Suffix	Y	N	N
Integrator AMXBeacon Mode	Y	N	N
Integrator Telepresence Mode	Y	N	N
IP Assignment	Y	Y	N
IP DNS Domain Name	Y	Y	N
IP DNS Server 1 through 5 Address	Y	Y	N
IP Gateway	Y	Y	N
IP SubnetMask	Y	Y	N
IPMedia MaxVideoTXRate	Y	Y	N
IPProtocol	Y	Y	N
IRControl Mode	Y	N	N
IRControl NumberKeyMode	Y	N	N
ISDN BRI Alert	Y	N	N
ISDN BRI AutoActivation	Y	N	N
ISDN BRI ChanId	Y	N	N
ISDN BRI Interface 1 through 6	Y	N	N
DirectoryNumber 1	Y	N	N
DirectoryNumber 2	Y	N	N
Mode	Y	N	N
SPID 1	Y	N	N
SPID 2	Y	N	N
ISDN BRI MaxDeactiveTime	Y	N	N
ISDN BRI SwitchType	Y	N	N

Field Name	Provisioned for supported Tandberg models?		
	MXP Models 990/880/770	MXP Model T150	C Series
ISDN CliNumbPlan	Y	N	N
ISDN CliNumbSpec	Y	N	N
ISDN CliNumbType	Y	N	N
ISDN HLC	Y	N	N
ISDN MSN	Y	N	N
ISDN ParallelDial	Y	N	N
ISDN PRI Alert	Y	N	N
ISDN PRI ChanId	Y	N	N
ISDN PRI InitialRestart	Y	N	N
ISDN PRI Interface HighChannel	Y	N	N
ISDN PRI Interface LowChannel	Y	N	N
ISDN PRI Interface MaxChannels	Y	N	N
ISDN PRI Interface NumberRangeStart	Y	N	N
ISDN PRI Interface NumberRangeStop	Y	N	N
ISDN PRI Interface Search	Y	N	N
ISDN PRI L2WindowSize	Y	N	N
ISDN PRI NSFTelephony Mode	Y	N	N
ISDN PRI NSFTelephony Number	Y	N	N
ISDN PRI NSFVideoTelephony Mode	Y	N	N
ISDN PRI NSFVideoTelephony Number	Y	N	N
ISDN PRI SwitchType	Y	N	N
ISDN SendComplete	Y	N	N
ISDN SendNumber	Y	N	N
ISDN SpeechTimers	Y	N	N
ISDN SubAddress	Y	N	N
Key AUX	Y	N	N

Field Name	Provisioned for supported Tandberg models?		
	MXP Models 990/880/770	MXP Model T150	C Series
Key Brightness	N	Y	N
Key Cabinet	Y	N	N
Key CallRegister	N	Y	N
Key Cancel	Y	Y	N
Key Connect	Y	Y	N
Key Disconnect	Y	Y	N
Key DocCam	Y	N	N
Key Down	Y	Y	N
Key FarEnd	Y	N	N
Key Grab	Y	N	N
Key Headset	N	Y	N
Key Help	Y	Y	N
Key Layout	Y	N	N
Key Left	Y	Y	N
Key MainCam	Y	N	N
Key MicOff	Y	Y	N
Key Number0 through Number9	Y	Y	N
Key Ok	Y	Y	N
Key PC	Y	N	N
Key Phonebook	Y	Y	N
Key PIP	N	Y	N
Key Presentation	Y	N	N
Key Presets	Y	N	N
Key Right	Y	Y	N
Key Selfview	Y	Y	N
Key Services	Y	Y	N
Key Settings	N	Y	N
Key Softkey1	N	Y	N

Field Name	Provisioned for supported Tandberg models?		
	MXP Models 990/880/770	MXP Model T150	C Series
Key Softkey2	N	Y	N
Key Softkey3	N	Y	N
Key Softkey4	N	Y	N
Key Softkey5	N	Y	N
Key Speaker	N	Y	N
Key Square	Y	Y	N
Key Star	Y	Y	N
Key Up	Y	Y	N
Key VideoOff	N	Y	N
Key VCR	Y	N	N
Key VolumeDown	Y	Y	N
Key VolumeUp	Y	Y	N
Key ZoomIn	Y	N	N
Key ZoomOut	Y	N	N
Keyboard Layout	Y	N	N
Kiosk AllowIRControl	Y	N	N
Kiosk AutoDial	Y	N	N
Kiosk LanguageMenu English	Y	N	N
Kiosk LanguageMenu French	Y	N	N
Kiosk LanguageMenu German	Y	N	N
Kiosk LanguageMenu Italian	Y	N	N
Kiosk LanguageMenu Mode	Y	N	N
Kiosk LanguageMenu Norwegian	Y	N	N
Kiosk LanguageMenu Spanish	Y	N	N
Kiosk LanguageMenu Swedish	Y	N	N
Kiosk Menu	Y	N	N
Kiosk Mode	Y	N	N
Kiosk OneClickConnect	Y	N	N

Field Name	Provisioned for supported Tandberg models?		
	MXP Models 990/880/770	MXP Model T150	C Series
Kiosk Phonebook	Y	N	N
LocalLayout Mode	Y	N	N
LocalLayout Toggle	Y	N	N
Logo	Y	Y	N
LoS Duration Exponent	Y	N	N
LoS Duration Offset	Y	N	N
LoS Inhibit	Y	N	N
LoS Initial	Y	N	N
LoS Polarity	Y	N	N
LoS Retry	Y	N	N
MainVideoSource	Y	N	N
MaxBandwidth	Y	N	N
Multipoint Mode	Y	N	N
Multipoint MultiwayMultiprotocol	Y	N	N
Multipoint MultiwayStartupPeriod	Y	N	N
Multipoint MultiwayURI	Y	N	N
NAT Address	Y	Y	N
NAT Mode	Y	Y	N
NetProfile 1 through 7	Y	Y	N
CallPrefix	Y	Y	N
CallSuffix	Y	N	N
Name	Y	Y	N
NTP Address	Y	Y	N
NTP Mode	Y	Y	N
OneClickConnect Mode	N	Y	N
OSD CallDuration Mode	Y	Y	N
OSD Icon BadNetwork	Y	N	N
OSD Icon CameraTracking	Y	N	N

Field Name	Provisioned for supported Tandberg models?		
	MXP Models 990/880/770	MXP Model T150	C Series
OSD Icon DuoVideo	Y	N	N
OSD Icon Encryption	Y	N	N
OSD Icon Headset	Y	N	N
OSD Icon MicOff	Y	N	N
OSD Icon OnAir	Y	N	N
OSD Icon Telephone	Y	N	N
OSD Icon VolumeOff	Y	N	N
OSD MCUStatusLine Mode	Y	N	N
OSD Menu BalloonHelp	Y	N	N
OSD Menu CodecLabel	Y	N	N
OSD Menu DisableH323IdCalling	N	Y	N
OSD Menu DisableTimeout	Y	Y	N
OSD Menu DisplayWelcomeText	Y	Y	N
OSD Menu DisplayWelcomeTime	Y	N	N
OSD Menu IconPlacement	Y	N	N
OSD Menu InputEditor Language	Y	N	N
OSD Menu Language	Y	Y	N
OSD Menu Mode	Y	Y	N
OSD Menu Password	Y	Y	N
OSD Menu Simple	Y	N	N
OSD Menu WelcomeMenu	Y	N	N
OSD Menu WelcomeText	Y	Y	N
OSD Mode	Y	N	N
OSD Offset Mode	Y	N	N
PacketlossDownSpeed Mode	Y	Y	N
PCPort Mode	N	Y	N
PictureProgram 1 Layout	Y	N	N

Field Name	Provisioned for supported Tandberg models?		
	MXP Models 990/880/770	MXP Model T150	C Series
PictureProgram 1 Window 1 through 6 Call	Y	N	N
PictureProgram 1 Window 1 through 6 Picture	Y	N	N
PictureProgram 2 Layout	Y	N	N
PictureProgram 2 Window 1 through 6 Call	Y	N	N
PictureProgram 2 Window 1 through 6 Picture	Y	N	N
PictureProgram 3 Layout	Y	N	N
PictureProgram 3 Window 1 through 6 Call	Y	N	N
PictureProgram 3 Window 1 through 6 Picture	Y	N	N
PictureProgram 4 Layout	Y	N	N
PictureProgram 4 Window 1 through 6 Call	Y	N	N
PictureProgram 4 Window 1 through 6 Picture	Y	N	N
PresentationStart	Y	N	N
Preset 1 through 15 Name	Y	N	N
QoS Diffserv Telephony Audio	Y	Y	N
QoS Diffserv Telephony Signalling	Y	Y	N
QoS Diffserv VideoTelephony Audio	Y	Y	N
QoS Diffserv VideoTelephony Data	Y	N	N
QoS Diffserv VideoTelephony Signalling	Y	Y	Y
QoS Diffserv VideoTelephony Video	Y	Y	Y
QoS Mode	Y	Y	Y
QoS Precedence Telephony Audio	Y	Y	Y
QoS Precedence Telephony Signalling	Y	Y	Y

Field Name	Provisioned for supported Tandberg models?		
	MXP Models 990/880/770	MXP Model T150	C Series
QoS Precedence VideoTelephony Audio	Y	Y	Y
QoS Precedence VideoTelephony Data	Y	N	Y
QoS Precedence VideoTelephony Signalling	Y	Y	Y
QoS Precedence VideoTelephony Video	Y	Y	Y
QoS RSVP	Y	Y	Y
QoS ToS	Y	Y	Y
RemoteSwUpgrade Mode	Y	N	Y
RemoteSwUpgrade Password	Y	N	Y
RTP MTU	Y	Y	Y
RTP Ports	Y	Y	Y
Screensaver Delay	Y	Y	Y
Screensaver LED	N	Y	Y
Screensaver Mode	Y	Y	Y
SecurityLog Mode	Y	N	Y
SelfViewOnStartup	Y	Y	Y
SerialPort 1 BaudRate	Y	N	Y
SerialPort 1 DataBits	Y	N	Y
SerialPort 1 Mode	Y	N	Y
SerialPort 1 Parity	Y	N	Y
SerialPort 1 StopBits	Y	N	Y
SerialPort 2 BaudRate	Y	N	Y
SerialPort 2 DataBits	Y	N	Y
SerialPort 2 Mode	Y	N	Y
SerialPort 2 Parity	Y	N	Y
SerialPort 2 StopBits	Y	N	Y

Field Name	Provisioned for supported Tandberg models?		
	MXP Models 990/880/770	MXP Model T150	C Series
SerialPort Direct Buffer	Y	N	Y
SIP Authentication Password	Y	Y	Y
SIP Authentication UserName	Y	Y	N
SIP Legacy Mask	Y	Y	N
SIP Mode	Y	Y	N
SIP ReplyTo URI	Y	N	N
SIP Server Address	Y	Y	N
SIP Server Discovery	Y	Y	N
SIP Server Type	Y	Y	N
SIP TLS Verify	Y	Y	N
SIP Transport Default	Y	Y	N
SNMP CommunityName	Y	Y	N
SNMP HostIPAddr 1	Y	Y	N
SNMP HostIPAddr 2	Y	Y	N
SNMP HostIPAddr 3	Y	Y	N
SNMP Mode	Y	Y	N
SNMP SystemContact	Y	Y	N
SNMP SystemLocation	Y	Y	N
SSH Mode	Y	Y	N
StartupVideoSource	Y	N	N
StillImageSource	Y	N	N
Streaming Address	Y	N	N
Streaming AllowRemoteStart	Y	N	N
Streaming Announcements	Y	N	N
Streaming Hops	Y	N	N
Streaming Password	Y	N	N
Streaming Port	Y	N	N
Streaming Quality	Y	N	N

Field Name	Provisioned for supported Tandberg models?		
	MXP Models 990/880/770	MXP Model T150	C Series
Streaming Source	Y	N	N
Streaming VideoRate	Y	N	N
StrictPassword	Y	Y	N
Switch Configuration Primary	Y	N	N
Switch Configuration Secondary	Y	N	N
Switch LogicalInput 1 Map	Y	N	Y
Switch LogicalInput 1 Mode 1	Y	N	Y
Switch LogicalInput 1 Mode 2	Y	N	Y
Switch LogicalInput 1 Mode 3	Y	N	N
Switch LogicalInput 1 Mode 4	Y	N	N
Switch LogicalInput 1 Mode 5	Y	N	N
Switch LogicalInput 2 Map	Y	N	N
Switch LogicalInput 2 Mode 1	Y	N	N
Switch LogicalInput 3 Map	Y	N	N
Switch LogicalInput 3 Mode 1	Y	N	N
Switch LogicalInput 4 Map	Y	N	N
Switch LogicalInput 4 Mode 1	Y	N	N
Switch LogicalInput 5 Map	Y	N	N
Switch LogicalInput 5 Mode 1	Y	N	N
Switch Source	Y	N	N
SystemUnit Multiway	N	Y	N
SystemUnit Password	Y	Y	N
T1 Interface CableLength	Y	N	N
Telnet Mode ^a	Y	Y	N
TelnetChallenge Mode	Y	Y	N
TelnetChallenge Port	Y	Y	N
Time DateFormat	Y	Y	N
Time DaylightSavings	Y	Y	N

Field Name	Provisioned for supported Tandberg models?		
	MXP Models 990/880/770	MXP Model T150	C Series
Time TimeFormat	Y	Y	N
Time Zone	Y	Y	N
UseAsLocalPCMonitor	Y	N	N
Video 1 Outputs Animation	Y	N	N
Video 1 Outputs Testpattern	Y	N	N
Video Inputs Source 1 through 6	Y	N	N
Name	Y	N	N
Quality	Y	N	N
Video Outputs DVI 1 and 2	Y	N	N
Mode	Y	N	N
OSD	Y	N	N
VirtualMonitor	Y	N	N
Video Outputs DVIResolution	Y	N	N
Video Outputs Letterbox	Y	N	N
Video Outputs ScreenFormatPC	Y	N	N
Video Outputs ScreenFormatTV	Y	N	N
Video Outputs TV 1 and 2	Y	N	N
Mode	Y	N	N
OSD	Y	N	N
VirtualMonitor	Y	N	Y
VNC DisplayNumber	Y	N	N
VNC IPAddress	Y	N	N
VNC Password	Y	N	N
WLAN Community	Y	N	N
WLAN Enable	Y	N	N
WLAN Encryption	Y	N	N
WLAN Key 1	Y	N	N
WLAN Key 2	Y	N	N

Field Name	Provisioned for supported Tandberg models?		
	MXP Models 990/880/770	MXP Model T150	C Series
WLAN Key 3	Y	N	N
WLAN Key 4	Y	N	N
WLAN Mode	Y	N	Y
WLAN SSID	Y	N	N
WLAN UseKey	Y	N	N

- a. The CMA system always provisions Telnet Mode to ON, because provisioning Telnet Mode to OFF would make the endpoints unmanageable.

Scheduled Provisioning of LifeSize Endpoints

The CMA system can provision many fields for LifeSize Team and Express endpoints. The following table identifies the fields that the CMA system can provision for LifeSize Team 200 endpoints. See the [“Endpoint Configuration/Provisioning”](#) on page 105 for information on implementing scheduled provisioning of endpoints.

Field Name	Provisioned for selected LifeSize Models?
	Team 200
Calls	
Outgoing Max BandWidth	Y
Incoming Max BandWidth	Y
Auto Bandwidth	Y
Maximum Call Time	Y
Maximum Redial Entries	Y
Auto Answer	Y
Auto Answer Mute	Y
Audio	
Audio Codecs	Y
Active Microphone	Y
Active Microphone Volume	Y

Field Name	Provisioned for selected LifeSize Models?
	Team 200
Primary Audio Output Test	Y
Audio Mute	Y
Muted Device(s)	Y
Video Call Audio Output	Y
Audio Call Audio Output	Y
Line Out Treble	Y
Line Out Bass	Y
Ring Tone Volume	Y
DMF Tone Volume	Y
Status Tone Volume	Y
Telepresence	
Telepresence	Y
HD Camera 1 Moment	Y
HD Camera 2 Moment	Y
Video Settings > Video Control	
Far Ctrl of Near Camera	Y
Far Set of Camera Presets	Y
Far Move to Camera Presets	Y
Camera Presets Lock	Y
Camera Pan Direction	Y
Default Primary Input	Y
Video Snapshots	Y
HD Camera 1 Name	Y
HD Input 1 Name	Y
Stretch Video	Y
Video Settings > Video Quality	
Video Bandwidth Balance	Y
Primary Video Motion	Y
Presentation Video Sharpness	Y

Field Name	Provisioned for selected LifeSize Models?
	Team 200
Video Encoder Quality	Y
H.241 MaxStaticMBPS	Y
Video MTU	Y
Security > General	
Telnet	Y
SNMP	Y
Security > Passwords	
SSH Password	Y
UI Admin Password	Y
UI User Password	Y
Network > General	
DHCP	Y
IP Address	Y
Subnet Mask	Y
Gateway	Y
Host Name	Y
DNS Server	Y
Name Search Domains	Y
Network Speed	Y
VLAN Tag	Y
NTP Server Host Name	Y
802.1x Authentication	Y
IPv6 Configuration	Y
IPv6 Address	Y
IPv6 Router	Y
Network > NAT	
Static NAT	Y
NAT Public IP Address	Y

Field Name	Provisioned for selected LifeSize Models?
	Team 200
Network > Reserved Ports	
UDP Lowest Value	Y
UDP Highest Value	Y
TCP Highest Value	Y
TCP Lowest Value	Y
Network > Network Qos	
Network QoS	Y
DiffServ Audio Priority	Y
DiffServ Video Priority	Y
DiffServ Data Priority	Y
InServ Audio Priority	Y
InServ Video Priority	Y
InServ Data Priority	Y
InServ ToS	Y
Network > LifeSize® Transit	
LifeSize® Transit	Y
Transit Hostname	Y
Transit Username	Y
Transit Password	Y
Transit ICE	Y
Transit Signaling	Y
Web Proxy URL	Y
Web Proxy Username	Y
Web Proxy Password	Y
Communications > General	
Auto Answer Multiway Calls	Y
Video Dialing	Y
Voice Dialing	Y
Presentations	Y

Field Name	Provisioned for selected LifeSize Models?
	Team 200
Auto Start Presentations	Y
Communications > H.323	
H.323	Y
H.323 Name	Y
H.323 Extension	Y
Gatekeeper ID	Y
Gatekeeper Mode	Y
Primary Gatekeeper IP and Port	Y
Alternate Gatekeeper IP and Port	Y
H.460	Y
Communications > SIP	
SIP	Y
SIP Username	Y
SIP Authorization	Y
SIP Server Type	Y
SIP Registration	Y
SIP Proxy	Y
SIP Proxy Host Name	Y
SIP Proxy Port	Y
SIP Registrar	Y
SIP Registrar Host Name	Y
SIP Registrar Port	Y
UDP Signaling	Y
UDP Signaling Port	Y
TCP Signaling	Y
TCP Signaling Port	Y
TLS Signaling	Y
TLS Signaling Port	Y

Field Name	Provisioned for selected LifeSize Models?
	Team 200
System > General	
Auto Reboot	Y
System > Identification	N
System Name	Y
Video Number	Y
Voice Number	Y
System > Identification	
Timezone	Y
Month	Y
Day	Y
Year	Y
Hour	Y
Minute	Y
Second	Y
Directory > Auto Discovery	
Auto Discovery	Y
Auto Discovery Subnets	Y
Auto Discovery Ignored Subnets	Y
Directory > LDAP	
LDAP	Y
LDAP Hostname	Y
LDAP Password	Y
LDAP Base	Y
LDAP Filter	Y
LDAP Refresh	Y
Appearance > General	
Language	Y
Fade Out Timeout	Y
Company Logo	Y

Field Name	Provisioned for selected LifeSize Models?
	Team 200
LCD Contrast	Y
Screen Saver	Y
Screen Saver Timeout	Y
Sleep Timeout	Y
Appearance > Layout	
Picture in Picture	Y
Display 2 Layout	Y
Appearance > Display	
Display 1 Resolution	Y
Display 1 Energy Saver	Y
Display 2 Energy Saver	Y
Display 2 Resolution	Y
Diagnostics > Cameras	
Camera Anti-Flicker	Y
HD Camera 1 Brightness	Y
HD Camera 1 White Balance	Y
HD Camera 2 White Balance	Y
HD Camera 2 Brightness	Y
Diagnostics > DVD-I Input	
DVI-I Input Horizontal Position	Y
DVI-I Input Vertical Position	Y
DVI-I Input Coarse Tuning	Y
DVI-I Input Fine Tuning	Y
DVI-I Input Brightness	Y
DVI_I Input Contrast	Y
DVI-I Input Scaling	Y

Provisioning of LifeSize Passwords

Take note of the following when provisioning passwords to LifeSize endpoints:

- The Auto password must be provisioned to meet the LifeSize and SSH/telnet rules for passwords.
- You cannot provision the Auto password to be blank. If you attempt to provision a blank value, the existing value of the password will not be overwritten. It will remain valid.
- The Web UI or User password can be provisioned to include the numbers 0-9 and/or the symbols * and #. The system will silently truncate these passwords to a maximum of 16 characters.
- You can provision the Web UI or User password to be blank.

Refer to the LifeSize documentation for more information about the requirements for these password.

Reporting

The CMA system includes standard reporting for select TANDBERG C Series, TANDBERG Edge, and LifeSize Team and Express endpoints.

Endpoint and Peripheral Management Operations

This chapter describes how to perform the Polycom® Converged Management Application™ (CMA®) system endpoint management tasks. It includes these topics:

- [Endpoint Management Operations](#)
- [Peripheral View Operations](#)

Endpoint Management Operations

The follow topics describe the actions available in **Endpoint > Monitor View**:

- [View Device Details](#)
- [Add an Endpoint or Find an Endpoint on the Network](#)
- [Edit an Endpoint](#)
- [Delete an Endpoint](#)
- [View an Endpoint's Video Feed](#)
- [Clear an Endpoint Help Request](#)
- [Send a Message to an Endpoint](#)
- [Reboot an Endpoint](#)
- [Associate a User with an Endpoint](#)
- [Search for Endpoints in a Range of IP Addresses](#)
- [View Peripherals](#)

View Device Details

To view detailed information about a managed endpoint

- 1 Go to **Endpoint > Monitor View**.
- 2 As needed, use the **Filter** to customize the endpoint list.
- 3 Select the endpoint of interest and click **View Details**.

The **Device Details** dialog box displays the following information:

Field	Description
Identification	
System Name	<p>The name of the endpoint.</p> <ul style="list-style-type: none"> Endpoint names must be unique. The name must be in ASCII only and may have an unlimited number of characters. Spaces, dashes, and underscores are valid. When retrieved from a video endpoint system, the name is taken from the H.323 ID if the endpoint registered with the gatekeeper and it is a third-party system. In other cases, it is the system name, which might be different than the H.323 ID.
Device Type	The type of endpoint. For valid types, see “Endpoint Types” on page 103.
IP Address	The assigned IP address of the endpoint.
Owner	The person to whom the endpoint is assigned.
Site	The network site for the endpoint. By default, endpoints are added to the Primary Site .
Product ID	The product model.
Description	A free-form text field (extended ASCII only) in which information about the endpoint can be added.
Serial Number	The serial number (ASCII only) of the endpoint. The endpoint provides the serial number if it registered successfully or is managed.
Software Version	The version of the software installed on the endpoint (ASCII only). The endpoint provides the version number if it registered successfully or is managed.

Field	Description
HTTP URL	<p>The management URL for the endpoint, if available (ASCII only). This URL allows the CMA system to start the endpoint's management system using the Manage function.</p> <p>All Polycom endpoints allow management through a browser. For these endpoints, this field is completed when the endpoint registers with the CMA system.</p>
HTTP Port	The HTTP port number for the endpoint. The endpoint provides the port number if it registered successfully and is managed.
Addresses	
SIP URI	<p>A SIP URI is the address used to call another person via SIP. In effect it's a user's SIP phone number. The SIP URI will be of the following format:</p> <p><i><username>@host(domain or IP):Port</i></p>
Aliases	<p>The aliases that allow you to connect to the endpoint. The CMA system converts the aliases to the IP address associated with the endpoint.</p> <ul style="list-style-type: none"> • Alias Type. Possible types include E.164, H.323 ID, URL, Transport Address, E-mail, Party Number, and Unknown. • Alias Value. Value for the alias type shown. • The value for the H.323 ID is the endpoint name if the endpoint registered with the gatekeeper and it is a third-party system. In other cases, the endpoint name is the system name, which might be different from the H323 ID. • The value of the E.164 alias is the extension dialed to reach this endpoint. <p>Notes</p> <ul style="list-style-type: none"> • To add aliases for the endpoint, edit the endpoint. • The following Alias Values are ASCII only: H323 ID, URL, Transport Address, and Unknown.
ISDN Video Number	<p>For ISDN endpoints only, the country code + city/area code + phone number for the endpoint.</p> <p>When you add an endpoint without native ISDN, the ISDN gateway, country code, and area code are not captured. The CMA system only supports native ISDN.</p>
LAN Host Name	The host name of the endpoint on the LAN. This can be different from the system name of the endpoint. It is an ASCII only name.
Call Signaling Address	The port on which the CMA system gatekeeper sends call signaling information.

Field	Description
RAS Address	The port on which the CMA system gatekeeper sends RAS addressing information.
Capabilities	
Supported Protocols	<p>The communications protocols that the endpoint can support. Possible values include:</p> <ul style="list-style-type: none"> IP (H.323) - A standard that defines the protocols used for multimedia communications on packet-based H.323 networks. IP (SIP) - A standard that defines the protocols used for multimedia communications on SIP networks. ISDN (H.320) - A standard that defines the protocols used for multimedia communications on switched networks, such as ISDN. <p>For endpoints with the type Unknown, select H.323. The endpoint automatically provides the protocols if it registered successfully or is managed.</p>
Required MCU Service	The MCU service selected for the endpoint to use.
Capabilities Enabled	<p>Capabilities enabled on this endpoint. Options are:</p> <ul style="list-style-type: none"> MCU - The endpoint can act as a control unit for multipoint conferences Gateway - The endpoint can act as a gateway for call management <p>The MCU provides the capability if it registered successfully or is managed.</p>
Monitoring Level	<p>The monitoring level for the endpoint. Possible values include:</p> <ul style="list-style-type: none"> Standard. This endpoint is monitored. VIP. This endpoint is monitored closely. The VIP identifier and filters are available to operators to monitor and manage conferences.
Available to Schedule	Identifies if the endpoint is available when users are scheduling conferences
Call Info > Sites	
Far Site Name	The H.323ID of the far site endpoint to which the selected endpoint is connected. When multiple endpoints are connected through the endpoint's embedded MCU, this field displays a concatenation of each endpoint's H.323ID separated by ' ', for example 'ISDN-CO1-7-1 Vsfx-9-1'.

Field	Description
Far Site Number	The address of the far site endpoint to which the selected endpoint is connected. The address value for the calling endpoint appears to be the dialed address. The address value for the called endpoint appears to be the IP Address.
Encryption	The type of encryption the far site uses.
Cause Code	The cause code showing how the call ended.
Error	
Video FEC Errors	The number of Forward Error Correction (FEC) errors that have been corrected in the current call.
Sync	
Call Type	Type of call, such as, H.323, SIP, ISDN, or POTS.
Call Info > Call Details	
Video Protocol	<p>The video connection protocol, both transmission (Tx) and reception (Rx), the endpoint is using. Possible values include:</p> <ul style="list-style-type: none"> • H.261—H.261 is an ITU standard designed for two-way communication over ISDN lines and supports data rates which are multiples of 64Kbit/s. H.261 supports CIF and QCIF resolutions. • H.263—H.263 is based on H.261 with enhancements that improve video quality over modems. It supports CIF, QCIF, SQCIF, 4CIF and 16CIF resolutions. • H.264
Video Format	The video format, both transmission (Tx) and reception (Rx), the endpoint is using.
Video Rate	The video bandwidth negotiated with the far site.
Video Rate Used	The actual video bandwidth used in the call to the far site.
Video Frame Rate	Specifies the frame rate the endpoint is using.
Audio Protocol	<p>The audio connection protocol, both transmission (Tx) and reception (Rx), the endpoint is using. Possible values include:</p> <ul style="list-style-type: none"> • G.711 • G.722 • G.728
Audio Rate	The audio bandwidth negotiated with the far site
Call Info > Quality of Service (Not reported by all endpoint types)	

Field	Description
Total Packet Loss	Specifies the total packet loss for the currently active call that is, the total percentage of packet loss for all currently active calls divided by the number of active calls.
% Packet Loss	Specifies the average percentage of packet loss for the currently active call that is, the total percentage of packet loss for all currently active calls divided by the number of active calls.
Audio Packet Loss	Specifies the audio packet loss for the currently active call.
Video Packet Loss	Specifies the video packet loss for the currently active call.
Audio Jitter	Specifies the audio jitter for the currently active call.
Video Jitter	Specifies the video jitter for the currently active call.
Call Info > Video Feed	
Near Site	The video feed from the endpoint.
Far Site	The video feed from the endpoint to which the endpoint is connected.
System Alerts	
Errors	Endpoint error message, for example, GK Registration error.
Warnings	Endpoint warning message, for example, Low Battery.

Add an Endpoint or Find an Endpoint on the Network

This topic describes how to manually add endpoints and how to find endpoints on the same network as the CMA system.

For most endpoints, you enter basic information. The CMA system then locates the endpoint and retrieves its information.

To add an endpoint to a CMA system or find an endpoint on the network

- 1 Go to **Endpoint > Monitor View** and click **Add** .

- 2 In the **Add New Device** dialog box, select the **Device Type**. For valid types, see “[Endpoint Types](#)” on page 103. For endpoints not specified in the list, select a **Device Type** of **Other**. This dialog is meant for adding endpoints that are managed in Standard Management mode.



Note

All dynamically-managed endpoints automatically register with the CMA system and cannot be added using the **Add** option.

- 3 Enter the **IP Address** of the endpoint.
- 4 Click **Find Device**.
 - If the CMA system can find the endpoint on the network, the **Add New Device** dialog box is populated with information retrieved from the endpoint. Review any information retrieved from the endpoint.
 - If the CMA system cannot find the endpoint on the network, a **Device Not Found** dialog box appears.



Notes

If you enter an invalid **Admin ID** or **Password** for an endpoint that requires that information, the CMA system may still find the endpoint. It depends upon the endpoint type.

- V-Series, VSX-Series, and Viewstation endpoints allow the CMA system to detect the endpoint type and complete the registration. The endpoint appears in the **Endpoint** list with an alert indicating **Incorrect Password**.
- Polycom HDX systems and ViewStation FX systems won't allow the CMA system to detect the endpoint type and complete the registration. You can manually add the endpoint, but the CMA system cannot communicate with it until you've entered a valid **Admin ID** or **Password** for the endpoint. In this case, the CMA system records an error message in an error log.
- The **Find Device** function only works for endpoints with a specified **Device Type**. If you selected a **Device Type** of **Other**, the CMA system will report an error.

- 5 Assign the endpoint a **System Name**.
Endpoint names must be unique, must be in ASCII only, and may have an unlimited number of characters. Spaces, dashes, and underscores are valid.
- 6 If necessary, enter the **Admin ID** and **Password** for the endpoint. Some endpoints may not require this information. Other endpoints may require only a password.
- 7 Complete the **Identification**, **Addresses**, and **Capabilities** sections of the **Add New Device** dialog box.

Pay particular attention to the **Capabilities** options, because the settings on it determine how the endpoint is used throughout the CMA system.

For example, you can select it as a **VIP** endpoint and determine whether it will be **Available to Schedule** through the scheduling interface.

Note that many fields in this dialog box are ASCII only. Depending on the selected type, some of these fields may not be displayed or may not be editable.

Field	Description
Identification	
Description	A free-form text field (extended ASCII only) in which information about the endpoint can be added.
GAB Display Name	Enter a name for the endpoint as it will appear in the Global Address Book.
Site	The network site for the endpoint. The system determines the site based upon IP address.
Serial Number	The serial number (ASCII only) of the endpoint. The endpoint provides the serial number if it registered successfully or is managed.
Software Version	The version of the software installed on the endpoint (ASCII only). The endpoint provides the version number if it registered successfully or is managed.
HTTP URL	<p>The management URL for the endpoint, if available (ASCII only). This URL allows the CMA system to start the endpoint 's management system using the Manage function.</p> <p>All Polycom endpoints allow management through a browser. For these endpoints, this field is completed when the endpoint registers with the CMA system.</p>
HTTP Port	The HTTP port number for the endpoint. The endpoint provides the port number if it registered successfully and is managed.
Addresses	
DNS Name	The name for the endpoint as entered on the domain name server.
SIP URI	<p>The address used to call the endpoint via SIP.</p> <p><i><username>@host(domain or IP):Port</i></p>

Field	Description
Aliases	<p>The aliases that allow you to connect to the endpoint. The CMA system converts the aliases to the IP address associated with the endpoint.</p> <ul style="list-style-type: none"> • Alias Type. Possible types include E.164, H.323 ID, URL, Transport Address, E-mail, Party Number, and Unknown. • Alias Value. Value for the alias type shown. <p>Notes</p> <ul style="list-style-type: none"> • The following Alias Values are ASCII only: H323 ID, URL, Transport Address, and Unknown. • The value for the H.323 ID is the endpoint name if the endpoint registered with the gatekeeper and it is a third-party system. In other cases, the endpoint name is the system name, which might be different from the H323 ID. • The value of the E.164 alias is the extension dialed to reach this endpoint.
ISDN Video Number	<p>For ISDN endpoints only, the country code + city/area code + local phone number for the endpoint.</p> <p>When you add an endpoint without native ISDN, the ISDN gateway, country code, and area code are not captured. The CMA system only supports native ISDN.</p>
Capabilities	
Supported Protocols	<p>The communications protocols that the endpoint can support. Possible values include:</p> <ul style="list-style-type: none"> • IP (H.323) - A standard that defines the protocols used for multimedia communications on packet-based H.323 networks. • IP (SIP) - A standard that defines the protocols used for multimedia communications on SIP networks. • ISDN (H.320) - A standard that defines the protocols used for multimedia communications on switched networks, such as ISDN. <p>For endpoints with the type Unknown, select H.323.</p> <p>The endpoint automatically provides the protocols if it registered successfully or is managed.</p>
Required MCU Service	The MCU service selected for the endpoint to use.

Field	Description
Capabilities Enabled	<p>Capabilities enabled on this endpoint. Options are:</p> <ul style="list-style-type: none"> • MCU - The endpoint can act as a control unit for multipoint conferences • Gateway - The endpoint can act as a gateway for call management <p>The MCU provides the capability if it registered successfully or is managed.</p>
Monitoring Level	<p>The monitoring level for the endpoint. Possible values include:</p> <ul style="list-style-type: none"> • Standard. This endpoint is monitored. • VIP. This endpoint is monitored closely. The VIP identifier and filters are available to operators to monitor and manage conferences.
Available to Schedule	Identifies if the endpoint is available when users are scheduling conferences

8 Click **Add**.

The endpoint appears in the **Endpoint** list. By default, the system may also:

- Add the endpoint to the applicable site.
- Set the **HTTP Port** to *80*
- Add an **Alias** for the endpoint.
- Make the endpoint **Available to Schedule**
- Set the **Monitoring Level** to **Standard**



Note


For third-party endpoints, the HTTP URL, serial number, and DNS name are not captured during endpoint registration.

Once you've added an endpoint, you can associate it with a user. See [“Assign Users Roles and Endpoints”](#) on page 272.

Edit an Endpoint

The CMA system automatically detects IP address changes and updates its database with the new information for Polycom and third-party endpoints that are registered with the CMA system.

To edit an endpoint in the CMA system

- 1 Go to **Endpoint > Monitor View**
- 2 As needed, use the **Filter** to customize the endpoint list.
- 3 Select the endpoint of interest and click **Edit** .
- 4 As required, edit the **Identification**, **Addresses**, and **Capabilities** sections of the **Edit Device** dialog box. For more information, see [“View Device Details”](#) on page 166.

Note that many fields in this dialog box are ASCII only.

- 5 Click **Update**.

**Note**

Editing information for an endpoint on the CMA system does not change the information in the endpoint. To make changes in the endpoint information, use **Provisioning** or change it at the endpoint interface. Note that for managed endpoints, the endpoint may overwrite settings entered manually.

Delete an Endpoint

To delete an endpoint from the CMA system

- 1 Go to **Endpoint > Monitor View**
- 2 As needed, use the **Filter** to customize the endpoint list.
- 3 Select the endpoint of interest and click **Delete**.
- 4 Click **Yes** to confirm the deletion.

The **Endpoint** list is updated.

**Note**

If your gatekeeper registration policy allows endpoints to register automatically with the CMA system (that is, a gatekeeper setting of **Allow Registration of All Endpoints** or **Allow Registration of Endpoints in Defined Sites** or **Allow Registration of Predefined Prefixes Only**) an endpoint that you delete may re-appear in the **Endpoint** list.

View an Endpoint's Video Feed



Note

This procedure is available on the following endpoint types:

- Polycom HDX system
- TANDBERG
- V-Series and VSX-Series
- ViewStation

To view the video feed for an endpoint (near site or far site)

- 1 Go to **Endpoint > Monitor View**
- 2 As needed, use the **Filter** to customize the **Endpoint** list.
- 3 Select the endpoint of interest and click **View Details**.

The **Device Details** dialog box appears. For information about these fields, see [“View Device Details”](#) on page 166.

- 4 Click **Call Info** to expand the **Call Info** options and select **Video Feed**.

The **Endpoint Video** section shows the video feed from the near and far site.

Clear an Endpoint Help Request

To clear an endpoint help request from the CMA system

- 1 Go to **Endpoint > Monitor View**
- 2 As needed, use the **Filter** to customize the **Endpoint** list.
- 3 Select the endpoint of interest and click **Clear Help**.

The **Confirm Endpoint Help Clear** dialog box appears.

- 4 To send a message to the endpoint as well as clear the help request, check **Also send message to endpoint**.
- 5 Click **Clear**.
- 6 If you selected the **Also send message to endpoint** check box, enter the text message to send the endpoint in the **Send Message to Endpoint** dialog box and click **Send**.

The **Endpoint** list is updated and alerts for the endpoint are cleared.



Note

If the reason for the original alert still exists on the endpoint, the alert will likely reappear in the **Endpoint** list.

Send a Message to an Endpoint

In some situations, such as in response to a help request, you can send a message to some types of endpoints.

To send a message to an endpoint from the CMA system

- 1 Go to **Endpoint > Monitor View**
- 2 As needed, use the **Filter** to customize the **Endpoint** list.
- 3 Select the endpoint of interest.
If the endpoint can receive text messages, a **Send Message** option appears in the **Action** menu.
- 4 Click **Send Message**.
- 5 In the **Send Message to Endpoint** dialog box, enter a text message and click **Send**.
The message is sent to the endpoint.

Reboot an Endpoint

In some situations, for example when a remote endpoint is unresponsive, you may need to reboot an endpoint remotely through the CMA system.

To reboot an endpoint from the CMA system

- 1 Go to **Endpoint > Monitor View**
- 2 As needed, use the **Filter** to customize the **Endpoint** list.
- 3 Select the endpoint of interest.
- 4 Click **Reboot Device**.
- 5 To confirm the request, click **Reboot**.

Associate a User with an Endpoint

To associate an endpoint to a user within the CMA system

- 1 Go to **Endpoint > Monitor View**
- 2 As needed, use the **Filter** to customize the **Endpoint** list.
- 3 Select the endpoint of interest.
- 4 Click **Associate User**.

- 5 In the **Last Name** field of the **Associate User** dialog box, enter all or part of the user's last name and click **Search**.
The system displays the list of users who meet your search criteria.
- 6 Select the user of interest and click **Close**.

Search for Endpoints in a Range of IP Addresses

To search for a set of endpoints within a range of IP addresses

- 1 Go to **Endpoint > Monitor View** and click **Search Devices**.
- 2 In the **Search Devices** dialog box, enter the starting IP address and ending IP address for the search range and click **Search**.

The system begins searching for endpoints. A progress bar displays the status of the search and a results message displays the number of endpoints searched and the number of endpoints found within the IP range.

View Peripherals

If an endpoint has one or more peripherals connected, you can view information about the peripherals.

- 1 Go to **Endpoint > Monitor View** and select an endpoint that has peripherals connected.
- 2 Click **View Peripherals**.
- 3 From the **Peripherals** dialog box, select the peripheral of interest to see the following information.

Field	Description
Status	The status shows if a paired peripheral is one of the following connection states: Connected Disconnected
Paired Endpoint	Name of the HDX or RealPresence Group Series endpoint that the peripheral is connected to.
Serial Number	The serial number of the peripheral.
IP Address	IP address of the peripheral, if applicable.
Hardware Version	Version of the peripheral hardware.
Software Version	Version of the peripheral software.

Peripheral View Operations

The following topics describe the actions available in the **Endpoint > Peripherals View**:

- [Delete Peripheral](#)
- [Display Applications](#)

Delete Peripheral

You can delete peripherals from the **Peripherals View** list when the peripheral is no longer connected to an endpoint.

- 1 Go to **Endpoint > Peripherals View** and select a peripheral that is listed as **Not Paired**.
- 2 Click **Delete Peripheral**.
- 3 In the **Confirm Delete** dialog box, click **Yes**.

Display Applications

For peripherals on which you can install multiple applications, you can display a list of installed applications and their version.

- 1 Go to **Endpoint > Peripherals View** and select a peripheral.
- 2 Click **Display Applications**.

The **Applications Installed on** dialog box for the selected peripheral appears.

Field	Description
Application Name	Name of the peripheral application.
Version	Version of the peripheral application.

- 3 Click **Close**.

Endpoint Provisioning Operations

This chapter discusses Polycom® Converged Management Application™ (CMA®) system automatic and scheduled endpoint provisioning operations.

It includes these topics:

- [Bundled Provisioning Operations](#)
- [Automatic Provisioning Operations](#)
- [Scheduled Provisioning Operations](#)

Bundled Provisioning Operations

This topic describes the bundled provisioning operations a user assigned the **Device Administrator** role can perform. These are:

- [View the Provisioning Bundle List](#)
- [Download a Provisioning Bundle](#)
- [Delete a Provisioning Bundle](#)

Bundled provisioning is not available when Maximum Security is enabled.

View the Provisioning Bundle List

To view the provisioning bundle list

- 1 Go to **Endpoint > Bundled Provisioning**.
- 2 As needed, use the **Filter** to customize the list of provisioning bundles.

Download a Provisioning Bundle

After you download a provisioning bundle for a specific HDX or RealPresence Group Series model, any dynamically managed HDX or RealPresence Group Series system of the same model will receive the provisioning bundle when an HDX or RealPresence Group Series system next polls the CMA system for new provisioning information.

If a provisioning bundle already exists for the model you select, the existing bundle is overwritten with the new one.

For more information about provisioning bundles, see [“Bundled Provisioning”](#) on page 106.

To download a provisioning bundle

- 1 Go to **Endpoint > Bundled Provisioning**.
- 2 Click **Download**.

The **Download Provisioning Bundle From an Endpoint** dialog lists all of the HDX and RealPresence Group Series systems registered with the CMA system.

- 3 As needed, use the **Filter** to customize the endpoint list.
- 4 Select an HDX or a RealPresence Group Series system that is configured the way you want for the provisioning bundle.
- 5 Complete the **Bundle Name** and **Description** fields.
- 6 Click **Download**.

The system confirms that the bundle downloaded successfully.

- 7 Click **OK**.

Delete a Provisioning Bundle

When you no longer need a provisioning bundle for an HDX or a RealPresence Group Series model, you can delete it. An existing provisioning bundle is also removed when you download a bundle for the same HDX or RealPresence Group Series model. The newly downloaded bundle overwrites the existing one.

- 1 Go to **Endpoint > Bundled Provisioning**.
- 2 As needed, use the **Filter** to customize the list of provisioning bundles.
- 3 Select the bundle you want to delete.
- 4 Click **Delete**.
- 5 Click **Yes** to confirm the deletion.

The system confirms that the bundle was deleted.

Automatic Provisioning Operations

This topic describes the automatic provisioning operations a user assigned the Device Administrator role can perform. These are:

- [View the Automatic Provisioning List and Details](#)
- [Add an Automatic Provisioning Profile](#)
- [Edit an Automatic Provisioning Profile](#)
- [Edit the Profile Order for an Automatic Provisioning Profile](#)
- [Clone an Automatic Provisioning Profile](#)
- [Delete an Automatic Provisioning Profile](#)

View the Automatic Provisioning List and Details

To view the automatic provisioning list and details about an automatic provisioning operation

- 1 Go to **Endpoint > Automatic Provisioning**.
- 2 As needed, use the **Filter** to customize the **Endpoint** list.
- 3 Select the endpoint of interest.
- 4 Expand the **Provisioning Details** tab in the **Device Details** section.

Add an Automatic Provisioning Profile

This topic describes how to add automatic provisioning profiles.




TIP

Add provisioning profiles in the middle of the work day, not first thing in the morning.

When you add an automatic provisioning profile, the CMA system immediately rolls it out. If it rolls it out first thing in the morning, people who need to attend a “start the day” conference will have to first wait for their endpoint to be provisioned. Better to implement profiles in the middle of the work day and then let the provisioning occur at the designated polling interval.

To add an automatic provisioning profile

- 1 Go to **Admin > Provisioning Profiles > Automatic Provisioning Profiles**.

- 2 In the **Automatic Provisioning Profiles** page, click **Add** .
- 3 In the **Add Profile** dialog box, enter a name for the profile and click **Next**.
- 4 Complete the **System Settings**, **Home Screen Settings**, **H.323 Settings**, **Call Settings**, **Audio Settings**, and (if applicable) **CMA Desktop Settings** sections of the **Provisioning Fields** dialog box.

For information about these fields, see “[Automatic Provisioning](#)” on page 107. The sections may differ depending on the endpoint type selected.

- 5 Click **OK**.


The provisioning profile appears at the bottom of the **Automatic Provisioning Profiles** list.

- 6 To change the priority order of the automatic provisioning profiles:
 - a Click in the **Profile Order** text box preceding the provisioning profile of interest and enter the priority for the profile.
 - b Click **Update Profile Order**.

The system assigns the provisioning profile the selected priority and shuffles and reassigns priorities to the other provisioning profiles.

Edit an Automatic Provisioning Profile

To edit an automatic provisioning profile

- 1 Go to **Admin > Provisioning Profiles > Automatic Provisioning Profiles**.
- 2 In the **Automatic Provisioning Profiles** page, select the profile of interest and click **Edit** .
- 3 Edit the **System Settings**, **Home Screen Settings**, **H.323 Settings**, **Call Settings**, **Audio Settings**, and (if applicable) **CMA Desktop Settings** sections of the **Provisioning Fields** dialog box.

For information about these fields, see “[Automatic Provisioning](#)” on page 107. The sections may differ depending on the endpoint type selected.

- 4 Click **OK**.

The provisioning profile is updated.

Edit the Profile Order for an Automatic Provisioning Profile


To edit the profile order for an automatic provisioning profile

- 1 Go to **Admin > Provisioning Profiles > Automatic Provisioning Profiles**.
- 2 In the **Automatic Provisioning Profiles** page, select the profile of interest, click in the **Profile Order** text box preceding the provisioning profile of interest, and enter the priority for the profile.
- 3 Click **Update Profile Order**.

The system assigns the provisioning profile the selected priority and shuffles and reassigns priorities to the other provisioning profiles.

Clone an Automatic Provisioning Profile

To clone an automatic provisioning profile


- 1 Go to **Admin > Provisioning Profiles > Automatic Provisioning Profiles**.
- 2 In the **Automatic Provisioning Profiles** page, select the profile of interest and click **Clone** .
- 3 In the **Clone Profile** dialog box, enter a name for the new profile and click **Save**.

The provisioning profile appears last in the **Automatic Provisioning Profiles** list.

- 4 As needed, edit the profile. See [“Edit an Automatic Provisioning Profile”](#) on page 184.

Delete an Automatic Provisioning Profile

To delete an automatic provisioning profile

- 1 Go to **Admin > Provisioning Profiles > Automatic Provisioning Profiles**.
- 2 In the **Automatic Provisioning Profiles** page, select the profile of interest and click **Delete** .
- 3 Click **Yes** to confirm the deletion.

The profile is deleted from the CMA system.

Scheduled Provisioning Operations

This topic describes the scheduled provisioning operations a user assigned the Device Administrator role can perform. These are:

- [View the Scheduled Provisioning List and Details](#)
- [Add a Scheduled Provisioning Profile](#)
- [Edit a Scheduled Provisioning Profile](#)
- [Clone a Scheduled Provisioning Profile](#)
- [Delete a Scheduled Provisioning Profile](#)
- [Schedule an Endpoint for Provisioning](#)
- [Check the Status of a Scheduled Provisioning](#)
- [Clear the Status of Scheduled Provisioning](#)
- [Cancel a Scheduled Provisioning](#)


View the Scheduled Provisioning List and Details

To view the automatic provisioning list and details about a scheduled provisioning operation

- 1 Go to **Endpoint > Scheduled Provisioning**.
- 2 As needed, use the **Filter** to customize the **Endpoint** list.
- 3 Select the endpoint of interest.
- 4 Expand the **Provisioning Details** tab in the **Device Details** section.

Add a Scheduled Provisioning Profile

To add a scheduled provisioning profile

- 1 Go to **Admin > Provisioning Profiles > Scheduled Provisioning Profiles**.
- 2 In the **Scheduled Provisioning Profiles** page, click **Add** .
- 3 In the **Add Profile** dialog box, select the **Endpoint Type** for the provisioning profile, enter a name for the profile, and click **Next**.

- 4 As needed, select **Provision This Page** and complete the **General Settings, Video Network, Monitors, Cameras, Audio Settings, LAN Properties**, and **Global Services** sections of the **Provisioning Fields** dialog box.

For information about these fields, see [“Scheduled Provisioning”](#) on page 113. The sections may differ depending on the endpoint type selected.

- 5 Click **OK**.

The provisioning profile appears in the updated **Scheduled Provisioning Profiles** list.

Edit a Scheduled Provisioning Profile

To edit a scheduled provisioning profile

- 1 Go to **Admin > Provisioning Profiles > Scheduled Provisioning Profiles**.
- 2 In the **Scheduled Provisioning Profiles** list, select the profile of interest and click **Edit Profile**.
- 3 As needed, select **Provision This Page** and complete the **General Settings, Video Network, Monitors, Cameras, Audio Settings, LAN Properties**, and **Global Services** sections of the **Provisioning Fields** dialog box.

For information about these fields, see [“Scheduled Provisioning”](#) on page 113. The sections may differ depending on the endpoint type selected.

- 4 Click **OK**.

The provisioning profile is updated.

Clone a Scheduled Provisioning Profile

To clone a scheduled provisioning profile

- 1 Go to **Admin > Provisioning Profiles > Scheduled Provisioning Profiles**.
- 2 In the **Scheduled Provisioning Profiles** page, select the profile of interest and click **Clone Profile**.
- 3 In the **Clone Profile** dialog box, enter a name for the new profile and click **Save**.

The provisioning profile appears first in the updated **Scheduled Provisioning Profiles** list.

- 4 Edit the sections of the **Provisioning Fields** dialog box. The sections and fields differ depending on the endpoint type selected. For more information on these fields, see the product documentation for the selected endpoint.
- 5 Review each page of the scheduled provisioning profile and determine if you want the parameters on the page provisioned. If you do want the parameters on the page provisioned, select **Provision This Page**.
- 6 Click **OK**.

The provisioning profile is updated.

Delete a Scheduled Provisioning Profile

To delete a scheduled provisioning profile

- 1 Go to **Admin > Provisioning Profiles > Scheduled Provisioning Profiles**.
- 2 In the **Scheduled Provisioning Profiles** page, select the profile of interest and click **Delete Profile**.
- 3 Click **Yes** to confirm the deletion.

The profile is deleted from the CMA system.

Schedule an Endpoint for Provisioning

To schedule an endpoint for provisioning

- 1 Go to **Endpoint > Scheduled Provisioning**.
- 2 As needed, use the **Filter** to customize the endpoint list.
- 3 Select the endpoints of interest.
- 4 Click **Provision**.
- 5 In the **Schedule Endpoint Provisioning** dialog box, select the appropriate provisioning profile.
- 6 In the **Schedule** field, select **Now** or **Later**.
- 7 If you select **Later**, enter a **Date** and **Time** for the provisioning.
- 8 Select either **Use Server Date/Time** or **Use Endpoint Date/Time** as these may differ.
- 9 Click **Schedule**.

The **Scheduled Provisioning View** reappears.

- 10 Click **Refresh**  and check the **Pending** column for the provisioning status.

For each endpoint you selected, the name of the profile appears in the **Pending** column, and the date and time you entered appears in the **Scheduled** column.

Check the Status of a Scheduled Provisioning

To check the status of a scheduled provisioning

- 1 Go to **Endpoint > Scheduled Provisioning**.
- 2 As needed, use the **Filter** to customize the endpoint list.
- 3 Select the endpoint of interest.
- 4 Expand the **Provisioning Details** tab in the **Device Details** section.

For information about the fields in this section, see [“View the Scheduled Provisioning List and Details”](#) on page 186.

Clear the Status of Scheduled Provisioning

To clear the status of a scheduled provisioning

- 1 Go to **Endpoint > Scheduled Provisioning**.
- 2 As needed, use the **Filter** to customize the endpoint list.
- 3 Select the endpoints of interest.
- 4 Click **Clear Status**.

The endpoint provisioning status returns to **Clear**.

Cancel a Scheduled Provisioning

You can only cancel provisioning of a **Pending** process. You cannot cancel the provisioning of an endpoint while it is **In Progress**.

To cancel a pending scheduled provisioning

- 1 Go to **Endpoint > Scheduled Provisioning**.
- 2 As needed, use the **Filter** to customize the endpoint list.
- 3 Select the endpoints of interest.

4 Click **Cancel Provision.**

The provisioning operation is cancelled and the provisioning status returns to **Clear**.

Endpoint Software Update Operations

This chapter describes how to use Polycom® Converged Management Application™ (CMA®) system to update the software on Polycom endpoints when a new software package is available. It includes these sections:

- [Automatic Software Update Operations](#)
- [Scheduled Software Update Operations](#)

Automatic Software Update Operations

For automatic software update, it includes these topics:

- [View Automatic Software Update Information](#)
- [View Automatic Software Update Packages](#)
- [Set Maintenance Window for Automatic Software Updates](#)
- [Implement Automatic Software Updates for Endpoints](#)
- [View and Implement Software Updates for Peripherals](#)

View Automatic Software Update Information

To view information for endpoints that are eligible for automatic software updates

- 1 Go to **Endpoint > Automatic Software Update**.
The **Automatic Software Update** page appears.
- 2 As needed, use the **Filter** to customize the endpoint list. Filter choices include **Type**, **Name**, **IP Address**, **ISDN Video Number**, **Alias**, and **Site**.
- 3 Select the endpoint of interest.

- 4 In the **Device Details** section, expand the **Software Update Details** tab. For more information, see [“Software Update Details”](#) on page 219.

View Automatic Software Update Packages

To view the list of automatic software update packages

- 1 Go to **Admin > Software Updates > Automatic Software Updates**.

The **Automatic Software Updates** page appears and the Polycom HDX Series automatic software update packages are displayed. The **Automatic Software Updates** page includes this information.

Field	Description
Version to use	Displays the default automatic software update profile to be used for the endpoint type and model.
Allow this version or newer	When checked, indicates that when a newer automatic software update package for the endpoint type and model is added, that package should be used as the default package.
Endpoint Type	The type of endpoint system. For valid endpoint system types, see “Endpoint Configuration/Provisioning” on page 105.
Version	The version of the software package associated with the automatic software update package.
Description	The meaningful name given to the automatic software update package when it was created.
Uploaded	The date and time when the automatic software update package was created.
Trial Group	The trial group assigned to the software update package, if applicable.

- 2 To view the Polycom CMA Desktop automatic software update packages, click the **CMA Desktop** tab.

Set Maintenance Window for Automatic Software Updates

You can restrict automatic software updates of dynamically-managed endpoint systems to a scheduled maintenance window.

Typically, automatic software updates occur as specified by the **Software Update Polling Interval** (**Admin > Site > Edit Site Provisioning Details > Provisioning Settings**). Enabling the maintenance window feature in the CMA system overrides the **Software Update Polling Interval**. The CMA system provisions the maintenance window to the endpoints, and the endpoints hold their automatic software update requests until the maintenance window starts.

Some notes about this feature:

- It applies to dynamically-managed HDX and RealPresence Group Series systems only.
- To avoid automatically updating the software on all HDX or RealPresence Group Series systems at the start of the maintenance window, the systems randomize their automatic software update requests.

To restrict automatic software updates to a scheduled maintenance window

- 1 Go to **Admin > Software Update > Automatic Software Update > Maintenance Window**.
- 2 In the **Maintenance Window** dialog box, click **Enable Maintenance Window** and set a maintenance window **Start Time** and either an **End Time** or **Duration**.

Set the maintenance window start time to the endpoint's system local time, not the CMA system local time. For example, if you set the maintenance window start time to 3am, the maintenance window for each HDX system will start at 3am local time. Therefore, the maintenance window for HDX systems in Buffalo, NY will start at 3am EST; the maintenance window for HDX systems in Denver, CO will start at 3am MST; and the maintenance window for HDX systems in San Francisco, CA will start at 3am PST.

- 3 Click **Save**.

Implement Automatic Software Updates for Endpoints


To implement automatic software updates, complete the following tasks:

- 1 [“List the Serial Numbers for the Endpoints to be Updated”](#) on page 194.
- 2 [“Download the Required Software Package”](#) on page 195.
- 3 [“Request Update Activation Keys”](#) on page 195.

- 4 [“Upload the Software Package and Create a Software Update Package”](#) on page 196. For more information on software update packages, see [“View Automatic Software Update Information”](#) on page 191.
- 5 [“Set an Automatic Software Update Policy”](#) on page 197.

List the Serial Numbers for the Endpoints to be Updated

To list the serial numbers for the endpoints to be updated

- 1 Go to **Admin > Software Updates > Automatic Software Updates**.
- 2 Click **Get Serial Numbers** .

The **Endpoint Serial Number List** appears listing the endpoints eligible for automatic software update. Endpoints without serial numbers and endpoints that are not actively managed by the system are excluded.
- 3 As needed, use the **Filter** to customize the endpoint list.
- 4 Select the specific endpoints to be updated. To select all endpoints in the list, click the check box in the column header.
- 5 Click **Get Serial Numbers**.

The serial number(s) appear in the text box on the page.

- 6 When updating a single endpoint:
 - a Record the serial number: _____
 - b Click **Close**.

The **Automatic Software Updates** list reappears.
 - c Go to [“Download the Required Software Package”](#) on page 195.
- 7 When updating multiple endpoints:
 - a Create a `.txt` file that you can submit to the **Polycom Product Activation** site. Put each License Number - Serial Number combination on a separate line as shown in the following example.

```
X1006-3202-3027-0101    VR207071500x
X1009-0453-6027-0202    VR207071500x
X1009-1624-6027-0303    VR207071500x
```

- b Return to the **Endpoint Serial Number List** and click **Close**.

The **Automatic Software Updates** list reappears.
- c Repeat steps 2 through 7 for each endpoint or set of endpoints to be updated. You may include all of the serial numbers for all of the different endpoint types in the same `.txt` file.
- d Save the `.txt` file.

- e Go to “[Download the Required Software Package](#)” on page 195.

Download the Required Software Package

To download the software package required to update the endpoint

- 1 On your local system, create a directory to which to save the software package (if one does not already exist).
- 2 For Polycom endpoints:
 - a Open a web browser and go to <http://support.polycom.com>.
 - b In the **Documents and Downloads** section, select the **Product Type** for the required software package (**Telepresence and Video** for video endpoints such as Polycom HDX systems or **Voice** for endpoints such as Polycom VVX systems).
 - c On the product listing page, click the link to the product page of interest.
 - d Select the software package and save it to the directory created in step 1.
 - e Repeat steps a through d for each endpoint type to be updated. Note that the software package may contain the software for different models of the same endpoint type.
- 3 For third-party endpoints, follow the company’s recommended procedure for downloading a software package. Save it to the directory created in step 1.

Request Update Activation Keys



Note

In general, you need an activation key when updating to a major release (for example, 3.x to 4.x) or minor release (for example, 3.1 to 3.2). You do not need an activation key when updating a point release (for example, 3.1.1 to 3.1.2). However, you should read the product release notes for specific information about whether or not you'll need an activation key.

To request upgrade activation keys

- 1 For Polycom endpoints, open a web browser and go to <http://support.polycom.com>.
- 2 In the **Licensing & Product Registration** section, select the **Activation/Upgrade**.
- 3 Log in or **Register for An Account**.

- 4 Select **Product Activation**.
- 5 To activate a single license:
 - a Click **SITE & Single Activation/Upgrade**.
 - b Enter the **Serial Number** and click **Next**.
 - c Read and click **Accept Agreement** to continue.
 - d Enter the **License Numbers** you received for the upgrade and click **Upgrade**.
 - e The key code is returned on the screen.
 - f Record the key code and create a `.txt` file with the Serial Number - Key Code combination to be updated.
- 6 To activate a batch of licenses:
 - a Click **Batch Activation**.
 - b Click **Browse** and browse to the location of the `.txt` file you created in step 7 on page 194.
 - c Click **Upload**.
A file containing the Serial Number - Key Code combinations will be E-mailed to the specified E-mail account.
 - d When you receive the `.txt` file, save it to your local system.
- 7 For third-party endpoints, follow the company's recommended procedure for requesting an upgrade activation key.

Upload the Software Package and Create a Software Update Package

After you receive notification about a new software package for a Polycom endpoint, upload the software update to the CMA system and create a software update profile to use for the update.



Note

When uploading a software package, log into the CMA system web interface using its fully qualified domain name (for example, CMAsystem.domain.com) rather than its IP address. As long as your browser did not display any certificate errors when logging in, you should be able to upload the software package successfully.

To upload the software package and create an automatic software update profile

- 1 Go to **Admin > Software Updates > Automatic Software Updates**.
- 2 Select the tab for the endpoint type of interest.
- 3 Click **Upload Software Update**.

- 4 In the **Upload Software Update** dialog box, verify the endpoint type and model.
- 5 If an activation key code is required to activate the software update, click the **Update Requires Key** check box and in the **Software Update Key File** field browse to the `.txt` key file received in “[Request Update Activation Keys](#)” on page 195.



Note

The key is generated from the endpoint serial number and version number, and Polycom sends it as a text (`.txt`) file to the customer when new software is available. Customers can review their key history at <http://support.polycom.com>.

- 6 Enter a meaningful description that will help other users to understand the purpose of the software update.
- 7 Click **OK**.

An automatic software update profile for the endpoint type and model type appears in the **Automatic Software Updates** list.

If you receive a message that indicates “This version is the first for its endpoint type, so it will be assumed to be the policy for this endpoint type,” the software update profile also appears in the **Version to use** field.

Set an Automatic Software Update Policy

To set an automatic software update policy for an endpoint type

- 1 Go to **Admin > Software Updates > Automatic Software Updates**.
- 2 Select the tab for the endpoint type of interest.
- 3 Choose one of these policies:
 - To specify a minimum version of automatic software update package, make that version the **Version to use** and select **Allow this version or newer**.
 - To require a specific version of automatic software update package, make that version the **Version to use** and clear **Allow this version or newer**.
 - To turn automatic software update off for an endpoint type, change the **Version to use** value to **(none)**.
- 4 Click **Update**.

Trial a Software Update Package

To trial a software update package:

- 1 Get the things you need to create the package. Complete these tasks:
 - a [“List the Serial Numbers for the Endpoints to be Updated”](#) on page 194.
 - b [“Download the Required Software Package”](#) on page 195.
 - c [“Request Update Activation Keys”](#) on page 195.
- 2 Set up testing. Complete these tasks:
 - a [“Create a Local Trial Group”](#) on page 198.
 - b [“Upload the Software Package and Create a Trial Software Update Package”](#) on page 199. For more information on software update packages, see [“View Automatic Software Update Information”](#) on page 191.
- 3 Once your testing of the trial software package is complete, do one of these tasks:
 - [“Promote the Trial Software Update Package to Production”](#) on page 199
 - [“Delete the Trial Software Update Package”](#) on page 200.

Create a Local Trial Group

To trial a software update with a specific group of local and/or enterprise users, create a local group that includes these users, as described in [“Add a Local Group”](#) on page 268. The people in this group will receive the trial software update package when their endpoint goes through its normal, automated software update process.



Notes

- You can use an existing enterprise group as a trial group, but you will not be allowed to change the enterprise group in any way.
- If the trial software group is a parent group with children, all of its children will inherit trial permissions.

Upload the Software Package and Create a Trial Software Update Package

To upload the software package and create a trial automatic software update package

- 1 Go to **Admin > Software Updates > Automatic Software Updates**.
- 2 Select the tab for the endpoint type of interest.
- 3 Click **Upload Software Update**.
- 4 In the **Upload Software Update** dialog box, verify the endpoint type and model.
- 5 If an activation key code is required to activate the software update, click the **Update Requires Key** check box and in the **Software Update Key File** field browse to the `.txt` key file received in [“Request Update Activation Keys”](#) on page 195.



Note

The key is generated from the endpoint serial number and version number, and Polycom sends it as a text (`.txt`) file to the customer when new software is available. Customers can review their key history at <http://support.polycom.com>.

- 6 Enter a meaningful description that will help other users to understand the purpose of the software update.
- 7 To trial the software with the group created previously, select **Trial Software** and from the **Select Trial Group** menu, select the trial group created in [“Create a Local Trial Group”](#) on page 198.
- 8 Click **OK**.

A trial automatic software update package for the endpoint type and model type appears in the **Automatic Software Update** list. You can tell it is a trial package, because the **Trial Group** column includes your entry.

The next time members of the trial group log into the system, their systems will be upgraded with the trial software package.

Promote the Trial Software Update Package to Production

If you determine that the trial software update package is acceptable for production, you can then promote it to production.

To promote a trial software update package to production

- 1 Go to **Admin > Software Updates > Automatic Software Updates**.

- 2 Select the tab for product to update.
- 3 Select the software update package of interest and click **Promote to Production**.
- 4 Click **Yes** to confirm the promotion.

The package becomes a production automatic software update package.

Delete the Trial Software Update Package

If you determine that the trial software update package is unacceptable for production, you can delete it.

To delete a trial software update package

- 1 Go to **Admin > Software Updates > Automatic Software Updates**.
- 2 Select the tab for product to update.
- 3 Select the software update package of interest and click **Delete Software Update**.
- 4 Click **Yes** to confirm the deletion.

The package is removed from the **Automatic Software Updates** list.

- 5 To return your trial group to the last production version of software, clear the **Allow this version or newer** option and click **Update**.
- 6 When all endpoints are back to the last production version of software, reset your automatic software update policy. See [“Set an Automatic Software Update Policy”](#) on page 197.

View and Implement Software Updates for Peripherals

For peripherals that permit software updates from the CMA system, you can download the updates from <http://support.polycom.com> and make them available from the CMA system web server. You also configure which updates are for trial or production use. The following topics describe software updates for peripherals:

- [View Software Updates for Peripherals](#)
- [Upload Peripheral Software Updates to the CMA Web Server](#)
- [Configure Peripheral Updates for Production](#)
- [Configure Peripheral Updates for Trial](#)



Note

When doing peripheral upgrades on redundant systems running Microsoft SQL Server 2005 or 2008 R1, you may receive an SQL server exception. To resolve this exception, upload the peripheral upgrade package to the secondary server as well.

View Software Updates for Peripherals

To view software updates for peripherals

- 1 Go to **Admin > Software Updates > Automatic Software Updates**.
- 2 Select the tab for a peripheral.

The tab includes this information.

Field	Description
Production URL	URL where the peripheral can access software updates configured for production use. The URL consists of the IP dress of the CMA system plus /repo.
Trial URL	URL where the peripheral can access software updates configured for trial use. The URL consists of the IP dress of the CMA system plus /repotrial.
Package Name	Displays the name of the software update package. Updates listed as platform are updates to the peripheral's operating system. Other updates are for specific applications.
Description	The meaningful name given to the software update package when it was created
Version	The version of the software package
Status	<p>The status of the software update. Possible values are:</p> <ul style="list-style-type: none"> • None - The software update has not been configured for production or trial. • Production - The software update is configured for production. It is available only from the Production URL. • Trial - The software update is configured for trial. It is available only from the Trial URL. • Both - The software update is configured for both production and trial. It is available from both the Production URL and the Trial URL.
Uploaded	The date and time when the software update package was uploaded

Upload Peripheral Software Updates to the CMA Web Server

After you download the software updates from <http://support.polycom.com> and save them on your hard drive, you can upload them to the CMA system web server.

To upload software updates to the CMA system web server

- 1 Go to **Admin > Software Updates > Automatic Software Updates**.
- 2 Select the tab for the peripheral.
- 3 Click **Upload Software Update**.
- 4 In the **Select File to Upload** dialog box, navigate to and select the software update that you saved to your hard drive.
- 5 Click **Open**.

The update is added to the list on the peripheral tab.



Note

If this is the first update for the platform or an application, the update is automatically configured for production.

Configure Peripheral Updates for Production

To configure software updates for production

- 1 Go to **Admin > Software Updates > Automatic Software Updates**.
- 2 Select the tab for the peripheral.
- 3 Click **Configure Production**.

The **Configure Production** dialog box includes the following information.

Field	Description
Configure Platform	
Platform Description	The meaningful name given to the platform software update package when it was created

Field	Description
Status	<p>The current status of the platform software update. Possible values are:</p> <ul style="list-style-type: none"> • None - The software update has not been configured as production or trial. • Production - The software update is configured as production. It is available only from the Production URL. • Trial - The software update is configured as trial. It is available only from the Trial URL. • Both - The software update is configured as both production and trial. It is available from both the Production URL and the Trial URL.
Configure Application	
Application Description	The meaningful name given to the application software update package when it was created
Platform Compatible	Column title shows the version of the currently selected platform. Use the drop-down list to select available application versions that match the platform version.
Status	<p>The current status of the application software update. Possible values are:</p> <ul style="list-style-type: none"> • None - The software update has not been configured as production or trial. • Production - The software update is configured as production. It is available only from the Production URL. • Trial - The software update is configured as trial. It is available only from the Trial URL. • Both - The software update is configured as both production and trial. It is available from both the Production URL and the Trial URL.

- 4 From the **Configure Platform** section, select the platform version to configure for production.

You can select only one platform version for production.

- 5 Click **Configure Application**.

- 6 For each application, select the version to configure for production from the **Platform Compatible** drop-down list.

The version selected must be compatible with the platform version listed in the column heading. If the application is not selected (no check mark), the application will not be configured for production.

7 Click **OK**.

From the peripheral itself, the configured software updates are now available using the **Production URL**.

Configure Peripheral Updates for Trial

To configure software updates for trial

- 1** Go to **Admin > Software Updates > Automatic Software Updates**.
- 2** Select the tab for the peripheral.
- 3** Click **Configure Trial**.

The **Configure Trial** dialog box includes the following information.

Field	Description
Configure Platform	
Platform Description	The meaningful name given to the platform software update package when it was created
Status	<p>The current status of the platform software update. Possible values are:</p> <ul style="list-style-type: none"> • None - The software update has not been configured as production or trial. • Production - The software update is configured as production. It is available only from the Production URL. • Trial - The software update is configured as trial. It is available only from the Trial URL. • Both - The software update is configured as both production and trial. It is available from both the Production URL and the Trial URL.
Configure Application	
Application Description	The meaningful name given to the application software update package when it was created
Platform Compatible	Column title shows the version of the currently selected platform. Use the drop-down list to select available application versions that match the platform version.

Field	Description
Status	<p>The current status of the application software update. Possible values are:</p> <ul style="list-style-type: none"> • None - The software update has not been configured as production or trial. • Production - The software update is configured as production. It is available only from the Production URL. • Trial - The software update is configured as trial. It is available only from the Trial URL. • Both - The software update is configured as both production and trial. It is available from both the Production URL and the Trial URL.

- 4 From the **Configure Platform** section, select the platform version to configure for trial.

You can select only one platform version for trial.

- 5 Click **Configure Application**.

- 6 For each application, select the version to configure for trial from the **Platform Compatible** drop-down list.

The version selected must be compatible with the platform version listed in the column heading. If the application is not selected (no check mark), the application will not be configured for trial.

- 7 Click **OK**.

From the peripheral itself, the configured software updates are now available using the **Trial URL**.

Scheduled Software Update Operations

For scheduled software update, it includes these topics:

- [View Scheduled Software Update Information](#)
- [View List of Software Update Packages](#)
- [Implement Scheduled Software Updates for Endpoints](#)

View Scheduled Software Update Information

To view information about software updates that are scheduled or for endpoints that are eligible for scheduled software updates

- 1 Go to **Endpoint > Scheduled Software Update**.
- 2 As needed, use the **Filter** to customize the endpoint list. Filter choices include **Type**, **Name**, **IP Address**, **ISDN Video Number**, **Alias**, and **Site**.
- 3 Select the endpoint of interest.
- 4 In the **Device Details** section, expand the **Software Update Details** tab. For more information, see [“Software Update Details”](#) on page 219.

View List of Software Update Packages

To view the list of scheduled software update packages

- Go to **Admin > Software Updates > Scheduled Software Updates**.
The **Scheduled Software Updates** page appears listing all of the endpoint types and models for which the CMA system can perform a scheduled software update. It includes this information. If a software update package has been uploaded to the system, the **Description** and **Uploaded** fields are populated for the endpoint.

Implement Scheduled Software Updates for Endpoints

To implement a scheduled software update, you must perform this series of tasks.

- 1 [“List the Serial Numbers for the Endpoints to be Updated”](#) on page 206.
- 2 [“Download the Required Software Package”](#) on page 207.
- 3 [“Request Update Activation Keys”](#) on page 195.
- 4 [“Upload the Software Package and Create a Software Update Package”](#) on page 196. For more information on software update profiles, see [“View Automatic Software Update Information”](#) on page 191.
- 5 [“Schedule the Software Update for Endpoints”](#) on page 209.

List the Serial Numbers for the Endpoints to be Updated

To list the serial numbers for the endpoints to be updated

- 1 Go to **Admin > Software Updates > Scheduled Software Updates**.

- 2 Select the appropriate **Endpoint Type** and **Endpoint Model** combination for the endpoint to update.

- 3 Click **Get Serial Numbers** .

The **Endpoint Serial Number List** appears listing the endpoints of the selected type and model that are eligible for scheduled software updates.

- 4 As needed, use the **Filter** to customize the endpoint list.
- 5 Select the specific endpoints to be updated. To select all endpoints in the list, click the check box in the column header.
- 6 Click **Get Serial Numbers**.

The serial number(s) appear in the text box on the page.

- 7 When updating a single endpoint:

- a Record the serial number: _____
- b Click **Close**.

The **Scheduled Software Updates** list reappears.

- 8 When updating multiple endpoints:

- a Copy and paste the serial numbers from the endpoint serial number list to a `.txt` file that you can submit to the **Polycom Product Activation** site. Put one serial number per line as shown in the following example.

```
82071007E1DACD
82070407E010CD
820418048078B2
82040903E00FB0
```

- b Return to the endpoint serial number list and click **Close**.

The **Scheduled Software Updates** list reappears.

- c Repeat steps 2 through 8 for the each endpoint or set of endpoints to be updated. You may include all of the serial numbers for all of the different endpoint types in the same `.txt` file.
- d Save the `.txt` file.

Download the Required Software Package

To download the software package required to update the endpoints

- 1 On your local system, create a directory to which to save the software package (if one does not already exist).
- 2 For Polycom endpoints:
 - a Open a web browser and go to <http://support.polycom.com>.

- b** In the **Downloads** section, select the **Product** and **Category** for the required software package.
 - c** Select the software package and save it to the directory created in step 1.
 - d** Repeat steps **a** through **d** for each endpoint type to be updated. Note that the software package may contain the software for different models of the same endpoint type.
- 3** For third-party endpoints, follow the company's recommended procedure for downloading a software package. Save it to the directory created in step 1.

Request Update Activation Keys

To request upgrade activation keys

- 1** For Polycom products
 - a** Go to ***http://support.polycom.com***.
 - b** Log in or **Register for An Account**.
 - c** Select **Product Activation**.
 - d** In the **Software Upgrade KeyCode** section, click **Retrieve Software KeyCode**.
 - e** When upgrading a single endpoint:
 - » Enter the serial number of the endpoint to be updated into the **Serial Number** field of the **Single Upgrade Key Code** section.
 - » Enter the version number to which you are upgrading and click **Retrieve**.
 - » The key code is returned on the screen.
 - » Record the key code and create a **.txt** file with the Serial Number - Key Code combination to be updated.
 - » Close the **Product Activation** screens.
 - f** When updating multiple endpoints from a prepared **.txt** file (step 7 on page 194):
 - » In the **Multiple Upgrade KeyCode** section, click **Add Attachment**.
 - » Browse to the location of the **.txt** file you created in step 7 on page 194 and click **Upload**.
 - » A file containing the Serial Number - Key Code combinations will be E-mailed to the specified E-mail account.
 - » When you receive the **.txt** file, save it to your local system.

- » Close the **Product Activation** screens.
- 2 For third-party endpoints, follow the company's recommended procedure for requesting an upgrade activation key.

Upload the Software Package and Create a Software Update Profile

To upload the software package and create an automatic software update profile

- 1 Go to **Admin > Software Updates > Scheduled Software Updates**.
- 2 On the **Software Update Profiles** list, click the check box to select the appropriate **Endpoint Type** and **Endpoint Model** combination for the endpoints to be updated. To select all endpoints in the list, click the check box in the column header.
- 3 In the **Upload Software Update** dialog box, verify the endpoint type and model.
- 4 If an activation key code is required to activate the software update, click **Update Requires Key** and in the **Software Update Key File** field browse to the `.txt` key file (received in "[Request Update Activation Keys](#)" on page 195).



Note

The key is generated from the endpoint serial number and version number, and Polycom sends it as a text (`.txt`) file to the customer when new software is available. Customers can review their key history at <http://support.polycom.com>.

- 5 Enter a meaningful description that will help other users to understand the purpose of the software update.
- 6 Click **OK**.
A scheduled software update profile for the endpoint type and model type is created.
- 7 In a redundant configuration, repeat steps 1 through 6 on the redundant server.

Schedule the Software Update for Endpoints

To schedule one or more endpoints for software update

- 1 Go to **Endpoint > Scheduled Software Update**.

- 2 As needed, use the **Filter** to customize the endpoint list.
- 3 Select the endpoints of interest and click **Software Update**.
- 4 In the **Schedule Software Update** dialog box, specify when the update should occur.
 - a In the **Schedule** field, select **Now** or **Later**.
 - b If you select **Later**, enter a **Date** and **Time** for the update.
 - c Select either **Use Server Date/Time** or **Use Endpoint Date/Time** as these may differ.
- 5 Select from these options.

Fields	Description
Remove address book entries	Select this check box to have all local address book entries removed after the update.
Remove system files	Select this check box to have all endpoint settings removed after the update. You must then reconfigure the endpoint.
Allow endpoint to be a DHCP server	Select this check box to allow the endpoint to be a DHCP server. Applies to V-Series, VSX-Series, and ViewStation endpoints only. For more information, see the endpoint's user guide.



Note

You may apply a single software update request to multiple endpoint models. If the request includes one or more scheduling options that are not valid for a selected endpoint model, the system applies only the options that are valid.

- 6 Click **Schedule**.

For each endpoint selected, the status changes to **Pending** and the date and time for the software update appears in the **Scheduled** column.

Cancel Software Updates

You can cancel scheduled software updates for an endpoint. You cannot explicitly cancel automatic software updates for an endpoint. You must do that at the endpoint.

To cancel scheduled software updates

- 1 Go to **Endpoint > Scheduled Software Update**.

- 2** As needed, use the **Filter** to customize the endpoint list.
- 3** Select the endpoint or endpoints of interest and click **Cancel Update**.

A confirmation dialog box appears. The dialog box may indicate that one or more of the selected endpoints had a software update in progress.

- 4** Click **Ok** to cancel in progress and future software updates for the selected endpoints and clear their status.

You can cancel software update operations that are in progress, but you may wish to check the endpoint afterward to verify it was left in a operational state.

Device Details

This chapter lists the fields found in the **Device Detail** section of the Polycom® Converged Management Application™ (CMA®) system interface. It includes these topics:

- [Device Summary Information](#)
- [Device Status Information](#)
- [Call Information](#)
- [Device Alerts Information](#)
- [Provisioning Details](#)
- [Software Update Details](#)

Device Summary Information

The **Device Summary** information in the **Device Details** section includes the following fields.

Field	Description
Name	The name of the device.
Type	The type of device. For valid device types, see "Endpoint Configuration/Provisioning" on page 105.
ID	The system-generated ID for the device.
Owner	(Endpoints only) The user associated with the device.
IP Address	The assigned IP address of the device.
Area	Area with which the device is associated.



Field	Description
ISDN Video Number	For ISDN devices only, the country code + city/area code + phone number for the device. When you add an endpoint without native ISDN, the ISDN gateway, country code, and area code are not captured. The CMA system only supports native ISDN.
Site	The network site for the device. By default, devices are added to the Primary Site .
Software Version	The version of the software installed on the device (ASCII only). The device provides the version number if it registered successfully or is managed.
Serial Number	The serial number (ASCII only) of the device. The device provides the serial number if it registered successfully or is managed.
Available to Schedule	Select this option to make the device available when users are scheduling conferences. Note The Available to schedule field is disabled for MGC and RMX devices.
Monitoring Level	(Endpoints only—grayed out for MCU devices.) The monitoring level for the device. Possible values include: <ul style="list-style-type: none"> Standard. This device is monitored. VIP. This device is monitored closely. The VIP identifier and filters are available to operators to monitor and manage conferences.
Supported Protocols	The communications protocols that the device can support. Possible values include: <ul style="list-style-type: none"> IP (H.323) - A standard that defines the protocols used for multimedia communications on packet-based networks, such as IP. ISDN (H.320) - A standard that defines the protocols used for multimedia communications on switched networks, such as ISDN. For devices with the type Unknown , select H.323 . The device automatically provides the protocols if it registered successfully or is managed. Notes <ul style="list-style-type: none"> If an endpoint is configured as a gateway (ISDN), only the H.323 check box is selected. If the endpoint supports true ISDN, the H.323 and ISDN check boxes are selected. RMX MCUs support only the H.323 protocol.

Field	Description
Capabilities Enabled	<p>Capabilities to enable on this device. Options are:</p> <ul style="list-style-type: none"> • MCU - The device can act as a control unit for multipoint conferences • Gateway - The device can act as a gateway for call management <p>The MCU provides the capability if it registered successfully or is managed.</p> <p>Note</p> <p>Currently, RMX MCUs cannot be Gateway devices.</p>
Alias (type)	<p>The alias to connect to the device. The CMA system converts the aliases to the IP address associated with the device.</p> <ul style="list-style-type: none"> • Alias Type. Possible types include E.164, H.323 ID, URL, Transport Address, E-mail, Party Number, and Unknown. • Alias Value. Value for the alias type shown.

Device Status Information

The **Device Status** information in the **Device Details** section includes the following fields.

Field	Description
Gatekeeper Registration	<p>The status of the device's registration with the gatekeeper service. Possible values include:</p> <ul style="list-style-type: none"> • Registered • Unregistered
Directory Registration	<p>The status of the device's registration with the Global Directory Service. Possible values include:</p> <ul style="list-style-type: none"> • Registered • Unregistered
Presence Registration	<p>The status of the device's registration with the presence service. Possible values include:</p> <ul style="list-style-type: none"> • Registered • Unregistered
Exchange Registration	<p>The status of the device's registration with the Microsoft Exchange service.</p>
SIP Registration	<p>The status of the device's registration with the SIP service.</p>

Field	Description
Device Managed	Indicates whether or not the CMA system is managing the device.
Last GK Registration	The date and time of the device's last gatekeeper registration in a default format of <i>mm-dd-yyyy hh:mm:ss AM / PM</i> with adjustment to the client-machine GMT offset
Device Local Time	The local time as set within the device in a default format of <i>hh:mm:ss AM / PM</i> . This field is blank for the following device types: MGC , RMX , GW/MCU , Other , and TANDBERG .
ISDN Line Status Type	<p>The status of the ISDN line. Possible values include:</p> <ul style="list-style-type: none"> Operational  Non-operations  <p>This field is blank for the following device types: PVX, MGC, RMX, GW/MCU, Other, and TANDBERG.</p>
ISDN Assignment Type	<p>How the ISDN type was assigned to the device. Possible values include:</p> <ul style="list-style-type: none"> Administrator, when the ISDN type was assigned manually by an administrator Endpoint, when the ISDN type was natively assigned in the endpoint Auto-Assigned, when the ISDN type was automatically assigned by the CMA system based on the site configuration From Network, when the ISDN type was derived from the gateway and extension Undefined, when the CMA system cannot identify the source for the ISDN type assignment <p>This field is blank for the following device types: PVX, MGC, RMX, GW/MCU, Other, and TANDBERG.</p>
Device ISDN Type	<p>The ISDN network interface type installed in the device. Possible values include:</p> <ul style="list-style-type: none"> ISDN_QUAD_BRI ISDN_PRI_T1 ISDN_BRI ISDN_UNKNOWN <p>This field is blank for the following device types: PVX, MGC, RMX, GW/MCU, Other, and TANDBERG.</p>

Call Information

The **Call Info** in the **Device Details** section includes the following fields.

Field	Description
Call Type	The connection protocol for the call in which the device is participating. Possible values include: H.323, H.320, and S.IP
Video Protocol	The video connection protocol, both transmission (Tx) and reception (Rx), the device is using. Possible values include: <ul style="list-style-type: none"> H.261—H.261 is an ITU standard designed for two-way communication over ISDN lines and supports data rates which are multiples of 64Kbit/s. H.261 supports CIF and QCIF resolutions. H.263—H.263 is based on H.261 with enhancements that improve video quality over modems. It supports CIF, QCIF, SQCIF, 4CIF and 16CIF resolutions. H.264
Video Format	The video format, both transmission (Tx) and reception (Rx), the device is using.
Audio Protocol	The audio connection protocol, both transmission (Tx) and reception (Rx), the device is using. Possible values include: <ul style="list-style-type: none"> G.711 G.722 G.728
Far Site Name	The H.323ID of the far site device to which the selected endpoint is connected. When multiple endpoints are connected through the device's embedded MCU, this field displays a concatenation of each endpoint's H.323ID separated by ' ', for example 'ISDN-CO1-7-1 Vsfx-9-1'.
Far Site Number	The address of the far site device to which the selected endpoint is connected. The address value for the calling device appears to be the dialed address. The address value for the called device appears to be the IP Address.
Cause Code	Standard H.323 cause code that reflects normal call termination or the nature of an internal failure, for example, '16' or '211'.
Encryption	The status of encryption for the call. Possible values include: Off, Disabled, AES, and DH-1024

Device Alerts Information

The **Device Alerts** information in the **Device Details** section includes the following fields.

Field	Description
Errors	Device error message text, for example, GK Registration error
Warnings	Device warning message text, for example, Low Battery

Provisioning Details

The **Provisioning Details** information in the **Device Details** section includes the following fields.

Field	Description
Last Profile Applied	The name of the last provisioning profile that was or was not successfully applied to the device. The Provisioning Status will be either Success or Failed .
Provisioning Status	<p>The device's current provisioning status. Possible values include:</p> <ul style="list-style-type: none">• Clear. No provisioning has been done.• Pending. Provisioning is scheduled for this device.• In Progress. The device is currently being provisioned.• Success. Provisioning has been completed successfully on this device.• Failed. Provisioning was not completed on this device. <p>Some endpoint systems expect all configuration fields to be provisioned. If any of the fields are not provisioned, the status will indicate failed. However, the endpoint will often function successfully.</p>
Pending Profile	<p>The name of the provisioning profile that is scheduled to be applied to the device. In this case, the Provisioning Status will be either Pending or In Progress.</p> <p>This field is blank if the device is not scheduled for provisioning.</p>
Scheduled	<p>The date and time, in the default format of <i>yyyy-mm-dd hh:mm</i>, when the device is scheduled to be provisioned.</p> <p>This field is blank if the device is not scheduled for provisioning.</p>

Field	Description
Last Attempt Date/Time	The date and time, in the default format of <i>yyyy-mm-dd hh:mm:ss</i> , of the last provisioning message exchanged with the device.
Failure Reason	<p>A text description of the reason the provisioning failed. Causes for failure include:</p> <ul style="list-style-type: none"> • The provisioning profile does not exist • The provisioning profile does not include provisioning information • The CMA system no longer manages the device • A password for the device is set in the video endpoint system, and you must enter it in the CMA system • The device is busy • A network error occurred • An incomplete transfer of provisioning information occurred • Provisioning has timed out • An internal error occurred on the device, and you must reboot it • An unknown error occurred. Reboot the device.
Log Message	A read-only text box that contains messages related to the device provisioning status

Software Update Details

The **Software Update Details** information in the **Device Details** section includes the following fields.

Field	Description
Software Update Status	<p>The device's software update status. Possible values include:</p> <ul style="list-style-type: none"> • Clear. A software update has not been done. • Pending. A software update has been scheduled and is pending. The device may be offline or in a call. • In Progress. The software update is in progress. • Success. A software update has completed successfully. • Failed. A software update could not be performed.

Field	Description
Scheduled	<p>The date and time, in the default format of <i>yyyy-mm-dd hh:mm</i>, when the device software is scheduled to be updated.</p> <p>This field is blank if the device is not scheduled for provisioning.</p>
Last Attempt Date/Time	<p>The date and time, in the default format of <i>yyyy-mm-dd hh:mm:ss</i>, of the last software update message exchanged with the device.</p>
Failure Reason	<p>A text description of the reason the software update failed. Causes for failure may include:</p> <ul style="list-style-type: none">• The software update file location does not exist.• A password for the device is set in the video endpoint system, and you must enter it in CMA.• A network error has occurred.• The update has timed out.• An internal error occurred on the device, and you must reboot it.• A profile has not been configured.• An endpoint is offline.• An incorrect activation key is in the key file.• An unknown error has occurred. Reboot the device
Log Message	<p>A read-only text box that contains the log message text recorded during the execution of the software update.</p> <p>Note that there are no log messages displayed for dynamically-managed endpoints.</p>

Network Device Management Overview

This chapter provides an overview of the Polycom® Converged Management Application™ (CMA®) system's network device management functions. It includes these topics:

- [Network Device Types](#)
- [Network Device Menu, Views, and Lists](#)

Network Device Types

A CMA system supports these network device types:

- Polycom MGC conferencing bridges
- Polycom RMX conferencing bridges
- Polycom Distributed Management Application™ (DMA®) systems
- Polycom Video Border Proxy (VBP) systems


Network Device Menu, Views, and Lists

The CMA system **Network Device** menu provides these views of the network device list:

- **Monitor View** – Displays the list of all manageable and registered network devices. Use this view to manage network devices.
- **VBPs** (Video Border Proxy systems) – Displays the list of Polycom VBP systems registered to the CMA system. Use this view to add, edit, or delete VBP systems.

- **MCUs** (Microprocessing Control Units) – Displays the list of Polycom MCUs (Polycom RMX or MGC conferencing platforms) registered to the CMA system. Use this view to add, edit, or delete MCUs.
- **DMAs** (Distributed Management Application systems) – Displays the list of Polycom DMA systems) registered to the CMA system. Use this view to add, edit, or delete DMA systems.

All of the **Network Device** views have the following information:

Section	Description
Views	The views you can access from the page
Actions	The set of available commands. The constant command in the Network Device views is Refresh  , which updates the display with current information.
Network Device List	The context-sensitive Network Device list for the selected view
Device Details	Information about the network device selected in the network device list including: <ul style="list-style-type: none"> • “Device Summary Information” on page 213 • “Device Status Information” on page 215 • “Call Information” on page 217 • “Device Alerts Information” on page 218 • “Provisioning Details” on page 218 • “Software Update Details” on page 219

Monitor View

Use the **Network Device > Monitor View** to monitor the network devices.







Network Device List in the Monitor View

By default, the **Network Device** list in the **Monitor View** displays a list of network devices the CMA system monitors, including those devices that registered automatically with the CMA system and those devices that were added manually for management and monitoring purposes.

The **Network Device** list in the **Monitor View** includes MCUs and Polycom DMA nodes. It does not include Polycom VBP devices.






The **Network Device** list in the **Monitor View** displays MCUs as two separate Device Types, the MCU type and a GW/MCU device. If automatic registration is allowed, individual H.323 cards and/or IP blades in Polycom MCUs are assigned the device type of **GW/MCU** during registration. This device type represents the cards’ network interface. If automatic registration is not allowed, you must add a **GW/MCU** device record for each H.323 card and IP blade.

The **Network Device** list has these fields.

Field	Description
Filter	<p>Use the filter choices to display other views of the Network Device list, which include:</p> <ul style="list-style-type: none"> • Type- Filters the list by device type. For more information, see “Network Device Types” on page 221. • Alerts- Filters the list by alert type: Help, Error, or Warning • Connection Status- Filters the list by connection status: In a Call, Online, or Offline • Name - Filters the list by system name entered • IP Address - Filters the list by IP address entered • Alias - Filters the list by the alias entered • Site - Filters the list by site location entered • Area - Available only when Areas are enabled. Filters the list by the area with which the device is associated.
Status	<p>The state of the network device. Possible values include:</p> <ul style="list-style-type: none"> • Online  • Offline  • In a call  • Unknown  • Device alert  • Gatekeeper registration error 
Name	The system name of the network device
Type	The type of network device. For valid device types, see “Network Device Types” on page 221.
IP Address	The IP address assigned to the network device
Site	The site to which the network device belongs
Alias	The alias assigned to the network device
Area	Available only when Areas are enabled. The area with which the network device is associated.

Actions in the Monitor View

Besides providing access to the network device views, the **Actions** section of the **Monitor View** may also include these context-sensitive commands depending on the selected device type.

Action	Use this action to...
Available for all device types	
Add 	Manually add a network device to the CMA system or find a network device on the network
View Details 	Display all of the Device Details for the selected network device
Edit 	Change connection settings for the selected network device. Note that if this is a managed device, the device may overwrite settings entered manually.
Delete 	Delete the selected network devices
Associate Area	Available only when Areas are enabled. Associate the selected network device to an area so that only specified users can manage it.
Available for only selected network device types	
Manage 	Open the selected network device's management interface in a separate browser window. This command is not available for the following device types: MGC , GW/MCU , and Other .

VBP View

Use the **VBP View** to manage Polycom Video Border Proxy™ (VBPTM) firewall devices on the network.

Polycom VBP devices, when installed at the edge of the operations center, secures critical voice, video, and data infrastructure components including VoIP softswitches, video gatekeepers, gateways, media servers, and endpoints.

The **VBP** list has the following information.

Field	Description
Name	A unique name to identify the Polycom VBP device.
Model	The model of Polycom VBP device.
Provider-side IP	The private network IP address for the Polycom VBP device.

Field	Description
Subscriber-side IP	The public network IP address for the Polycom VBP device.

MCU View

Use the **MCU View** to manage Polycom MCU conferencing platforms on the network.

The **MCU** list has the same fields as the **Network Device > Monitor** view. For more information, see “[Monitor View](#)” on page 222.

DMA View

The Polycom® Distributed Media Application (DMA) system is a multipoint conferencing manager that uses advanced routing policies to distribute voice and video calls among multiple media servers (Multipoint Control Units, or MCUs), creating a single virtual resource pool. This greatly simplifies video conferencing resource management and uses MCU resources more efficiently.

Use the **DMA View** to manage DMA systems v2.3 or earlier. These earlier versions of the DMA system register with the CMA system as a Gateway/MCU and can be displayed in the **DMA** list.

The **DMA** list has the following information.

Field	Description
Name	A unique name for the DMA system.
Virtual IP Address	The virtual IP address for the DMA system.
Dial Prefix	E.164 dial string prefix for calling the system. Must be unique among the gatekeeper's devices and services. For more information, see the <i>Polycom DMA 7000 System Operations Guide</i> .
Description	A useful description for the DMA system.



IMPORTANT

Newer versions of the DMA system (v3.0 or greater) include call server functionality (H.323 gatekeeper and SIP proxy/registrar). For that reason, these DMA systems do not register with the CMA system as a Gateway/MCU and should not be added to the CMA system as a network device. Instead, these DMA system should be added to the CMA system as a trusted neighbor.


MCU Bridge Management Operations

This chapter describes how to perform the Polycom® Converged Management Application™ (CMA®) system MCU bridge management tasks. It includes these topics:

- [View Device Details](#)
- [Add an MCU Manually](#)
- [Edit an MCU Bridge](#)
- [Delete an MCU Bridge](#)
- [View Bridge Hardware](#)
- [View Bridge Services](#)
- [View Bridge Conferences](#)
- [View Bridge Ports](#)
- [View Bridge Meeting Rooms](#)
- [View Bridge Entry Queues](#)
- [View Bridge Gateway Conferences](#)

View Device Details

To view detailed information about a managed MCU bridge

- 1 Go to **Network Device > MCUs**.
- 2 As needed, use the **Filter** to customize the MCU list.
- 3 Select the MCU of interest and click **View Details** .

The **Device Details** dialog box for the selected MCU appears.

Field	Description
Identification	
System Name	<p>The name of the MCU.</p> <ul style="list-style-type: none"> MCU names must be unique. The name must be in ASCII only and may have an unlimited number of characters. Spaces, dashes, and underscores are valid. When retrieved from the MCU, the name is taken from the H.323 ID if the MCU registered with the gatekeeper and it is a third-party system. In other cases, it is the system name, which might be different than the H.323 ID.
Device Type	The type of MCU. For valid types, see "Network Device Types" on page 221.
IP Address	The assigned IP address of the MCU
Site	The network site for the MCU. By default, MCUs are added to the Primary Site .
Product ID	
Description	A free-form text field (Extended ASCII only) in which information about the MCU can be added
Serial Number	The serial number (ASCII only) of the MCU. The MCU provides the serial number if it registered successfully or is managed.
Software Version	The version of the software installed on the MCU (ASCII only). The MCU provides the version number if it registered successfully or is managed.
HTTP URL	<p>(RMX MCUs only) The management URL for the endpoint, if available (ASCII only). This URL allows the CMA system to start the endpoint's management system using the Manage function.</p> <p>All Polycom endpoints allow device management through a browser. For these endpoints, this field is completed when the endpoint registers with the CMA system.</p> <p>For third-party endpoints that do not register using an IP address, you must enter the URL.</p>
HTTP Port	<p>(RMX MCUs only) The HTTP port number for the MCU communications. The MCU provides the port number if it registered successfully and is managed.</p> <p>By default, in non-secure (HTTP) mode, the RMX uses port 80 and in secure (HTTPS) mode, the RMX uses port 443.</p>

Field	Description
Addresses	
DNS Name	The DNS name for the MCU.
Aliases	<p>The aliases that allow you to connect to the MCU. The CMA system converts the aliases to the IP address associated with the MCU.</p> <ul style="list-style-type: none"> • Alias Type. Possible types include E.164, H.323 ID, URL, Transport Address, E-mail, Party Number, and Unknown. • Alias Value. Value for the alias type shown. • The value for the H.323 ID is the MCU name if the MCU registered with the gatekeeper and it is a third-party system. In other cases, the MCU name is the system name, which might be different from the H323 ID. <p>Notes</p> <ul style="list-style-type: none"> • To add aliases for the MCU, edit the MCU. • The following Alias Values are ASCII only: H323 ID, URL, Transport Address, and Unknown.
ISDN Video Number	The country code + city/area code + phone number for the MCU.
Capabilities	
Supported Protocols	<p>The communications protocols that the MCU can support. Possible values include:</p> <ul style="list-style-type: none"> • IP (H.323) - A standard that defines the protocols used for multimedia communications on packet-based networks, such as IP. • ISDN (H.320) - A standard that defines the protocols used for multimedia communications on switched networks, such as ISDN. <p>The MCU automatically provides the protocols if it registered successfully or is managed.</p>
Capabilities Enabled	<p>Capabilities to enable on this MCU. Options are:</p> <ul style="list-style-type: none"> • MCU - The device can act as a control unit for multipoint conferences • Gateway - (MGC MCUs only) The device can act as a gateway for call management <p>The MCU provides the capability if it registered successfully or is managed.</p>
Available to Schedule	Select this option to make the MCU available to users who are scheduling conferences
Monitoring Level	Not applicable to MCU devices.

Field	Description
MCU (Network) Services	
Service Type	<p>The available network services may include:</p> <ul style="list-style-type: none"> • H.323 Service—Indicates a connection to an IP network using the H.323 protocol. • H.320 Service—Indicates a connection to an ISDN phone line using the H.320 protocol. • Gateway Service—(MGC MCUs only) Indicates a connection to both IP and ISDN to enable conversion from one protocol to the other. • Direct Service—Indicates a direct connection between an MCU and a video endpoint system, using a serial cable.
Service Name	A descriptive name for the network service.
Priority	The priority set for the network service as compared to other services when it was created.
MCU Resources	
Max Total Conferences	Maximum number of total conferences allowed at once on this MCU.
Max CP Conferences	Maximum number of continuous presence (CP) conferences allowed, based on the number of licenses available.
Max Video Ports	(RMX MCUs only)
Max Total Participants	Maximum number of total MCU participants allowed at once on this MCU.
Max Transcoding Ports	(MGC MCUs only) Maximum number of transcoding ports on which both ISDN and IP participants can be connected.
Use Entry Queue	Indicates whether the MGC device supports an IVR.
Entry Queue Number ID	The IP number that conference participants dial to access the IVR prompt to join a conference.
Max Bandwidth Capacity (Kbps)	The maximum bandwidth supported by the Polycom RMX MCU.

Field	Description
Alerts (RMX MCUs only)	
Category	<p>Lists the type of error. The following categories may be listed:</p> <ul style="list-style-type: none"> • File – indicates a problem in one of the files stored on the MCU's hard disk. • Card – indicates problems with a card. • Exception – indicates software errors. • General – indicates a general error. • Assert – indicates internal software errors that are reported by the software program. • Startup – indicates errors that occurred during system startup. • Unit – indicates problems with a unit. • MPL - indicates an error related to a Shelf Management component (MPL component) other than an MPM, RTM or switch board.
Level	<p>Indicates the severity of the problem, or the type of event. There are three fault level indicators:</p> <ul style="list-style-type: none"> • Major Error • System Message • Startup Event
Code	Indicates the problem, as identified by the error category
Card Alerts (MGC MCUs only)	
Slot	<p>Displays an icon according to the HW component type and the slot number. The icon displays the hardware status as follows:</p> <ul style="list-style-type: none"> • An exclamation point (!) indicates errors in the HW component. • Card icon with the reset button () indicates that the HW component is currently resetting. • Card icon with diagnostic tools () indicates that the HW component is in diagnostic mode.
Type	The type of hardware card

Add an MCU Manually

This topic describes how to add an MCU to a CMA system.



Note

Back-end communication with the RMX control units and IP service blades must be enabled.

When you add an MCU device, MCU network services are added automatically at the time the IP card registers with the CMA system.

When you add a gateway device, use the **Services** page to specify the network services available for the device.




Notes

- Polycom RMX devices may only have H.323 service.
- Once an MCU registers with the CMA system, if you change an MCU service on the MCU, the update does not automatically get sent to the CMA system. To update the system, you must delete and read the MCU to the system.
- These network services are not the same as the **Dial Plan Services** such as **Simplified Dialing** and **Conference on Demand**. Network services describe the physical connection that the device supports. Dial plan services provide access to specific features used for routing calls by dialing a prefix.

When you enter network service information manually, remember that the CMA system does not create the service at the device. The service must have already been defined at the device. Enter information in the CMA system that matches the information in the device.

If you do not define network services, you may not use an MCU or gateway in a conference. For example, if you do not define the H.323 service on the MCU, when the CMA system tries to schedule a video conference that requires this service, it will look for another MCU with this service. If another MCU with this service is not available, the conference will not be scheduled.

To add an MCU bridge to a CMA system or find an MCU on the network

- 1 Go to **Network Device > MCUs** and click **Add** .
- 2 In the **Add New Device** dialog box, select the **Device Type** of interest. For valid types, see [“Network Device Types”](#) on page 221.
- 3 Enter the **IP Address** of the MCU.
- 4 Enter the **Admin ID** and **Password** for the MCU.

- 5 Click **Find Device**.
 - If the CMA system can find the MCU on the network, the **Add New Device** dialog box is populated with information retrieved from the MCU. Review any information retrieved from the MCU.
 - If the CMA system cannot find the MCU on the network, a **Device Not Found** dialog box appears.
- 6 Click **OK**.
- 7 Complete the **Identification, Addresses, Capabilities, MCU Services, MCU Resources, and MCU Cascading** sections of the **Add New Device** dialog box. (For more information, see [“View Device Details”](#) on page 227.) At a minimum, assign the MCU a **System Name**.



Note

When naming an RMX system, use lowercase letters to specify the FQDN in the **System Name** field.

Pay particular attention to the **Capabilities** options, because the settings on it determine how the MCU is used throughout the CMA system.

- 8 Click **Add**.

The MCU appears in the **Network Device** list. By default, the system:

- Adds the MCU to the applicable site
- Sets the **HTTP Port** to *80*
- Adds an **Alias** for the endpoint
- Makes the endpoint **Available to Schedule**
- Sets the **Monitoring Level** to **Standard**




Notes

- In the **Device List**, a CMA system displays a single MCU as two separate **Device Types** (an **RMX** or **MGC** device and a **GW/MCU** device). The GW/MCU designation represents the network interface.
- For third-party endpoints, the HTTP URL, serial number, and DNS name are not captured during endpoint registration.

Edit an MCU Bridge

To edit an MCU from the CMA system

- 1 Go to **Network Device > MCUs**.
- 2 As needed, use the **Filter** to customize the MCU list.

- 3 Select the MCU of interest and click **Edit** .
- 4 Complete the **Identification**, **Addresses**, **Capabilities**, **MCU Services**, **MCU Resources**, and **MCU Cascading** sections of the **Edit Device** dialog box. (For more information, see [“View Device Details”](#) on page 227.) At a minimum, assign the MCU a **System Name**.
- 5 Click **Update**.

Enable Cascading Conferences on Polycom MCUs

To enable multi-bridge conferences, you must complete the following steps:

- 1 Configure entry queues on the participating MCUs. Only bridges with entry queues are displayed in the list of available bridges to schedule on the people-to-bridge or bridge-to-bridge scheduling page.

To configure cascading using a Polycom RMX MCU, you must create two cascading entry queues—one for which the **Master** option on the **Cascade** menu is selected and one for which the **Slave** option on the **Cascade** menu is selected. Also, enable the **Use Entry Queue** selection.


The primary purpose for the Master and Slave designation is to determine which Polycom RMX MCU is responsible for managing People + Content for the conference.

- 2 Configure **MCU Cascading** for each MCU on the CMA system by editing each MCU and referencing the appropriate entry queue ID and ISDN numbers.

Some notes about cascading MCUs:

- A Polycom RMX 1000 MCU cannot be used for cascading.
- All devices (MCUs and endpoints) in a cascaded conference must be registered to the same CMA system gatekeeper.
- All systems (the CMA system, MCUs, and endpoints) must be time synchronized.
- Since ISDN cascade links on Polycom RMX MCUs are not supported, do not select **Enable ISDN/PSTN Access**. The CMA system only supports cascaded IP links on Polycom RMX MCUs. It does not support cascaded ISDN links on Polycom RMX MCUs.
- Polycom RMX systems enforce a 1x1 layout for the cascaded link between bridges, so only one participant on each bridge is displayed at any time. To change this on a Polycom RMX system, go to **Setup > System Configuration** and on the **MCMS_PARAMETERS_USER** page add a new flag called **FORCE_1X1_LAYOUT_ON_CASCADED_LINK_CONNECTION** with a **Value** of **NO**.

To enable cascading conferences

- 1 On the MCUs, configure entry queues as required and record the entry queue number(s). For more information, see the product documentation for the MCU.
- 2 Go to **Network Device > MCUs**.
- 3 As needed, use the **Filter** to customize the MCU list.
- 4 Select the MCU of interest and click **Edit** .
- 5 Go to the **MCU Resources** section of the **Edit Device** dialog box and select **Use Entry Queue**.
- 6 Go to the **MCU Cascading** section of the **Edit Device** dialog box.
- 7 For a Polycom RMX MCU:
 - a Enter the **Master Entry Queue Number ID** and **Slave Entry Queue Number ID**.
 - b (Optional) Enter the **Master Entry Queue ISDN Number** and **Slave Entry Queue ISDN Number**.
- 8 For a Polycom MGC MCU:
 - a Enter the **Cascade Entry Queue Number ID**.
 - b (Optional) Enter the **Cascade Entry Queue ISDN Number**.
- 9 Click **Update**.

Delete an MCU Bridge

To delete an MCU from the CMA system

- 1 Go to **Network Device > MCUs**.
- 2 As needed, use the **Filter** to customize the MCU list.
- 3 Select the MCU of interest and click **Delete**.
- 4 Click **Yes** to confirm the deletion.
The **MCU** list is updated.

View Bridge Hardware

To view the hardware configuration of a bridge

- 1 Go to **Network Device > MCUs**.

- 2 As needed, use the **Filter** to customize the MCU list.
- 3 In the MCU list, select the bridge of interest and click **View Hardware**.

A **Hardware** pane appears below the bridge list. It lists the hardware for the selected bridge and displays the **Slot number**, **Card Type**, **Status**, **Temperature**, and **Voltage** for each piece of hardware.

View Bridge Services

To view the network services available on the bridge

- 1 Go to **Network Device > MCUs**.
- 2 As needed, use the **Filter** to customize the MCU list.
- 3 In the MCU list, select the bridge of interest and click **View Services**.

A **Services** pane appears below the bridge list. It lists the network services for the selected bridge and identifies the **Service Type**, **Service Name**, and the default setting for the network service.

View Bridge Conferences

To view information about the conferences resident on the bridge

- 1 Go to **Network Device > MCUs**.
- 2 As needed, use the **Filter** to customize the MCU list.
- 3 In the MCU list, select the bridge of interest and click **View Conferences**.

A **Conferences** pane appears below the bridge list. It lists the conferences for the selected bridge and identifies the conference **Status**, **Type**, **Name**, **Start Time**, **Bridge**, and **Owner**.

View Bridge Ports

To view information about the bridge ports

- 1 Go to **Network Device > MCUs**.
- 2 As needed, use the **Filter** to customize the MCU list.

- 3 In the MCU list, select the bridge of interest and click **View Ports**.

A **Ports** pane appears below the bridge list. It lists the ports for the selected bridge and identifies the **Audio Ports Available**, **Video Ports Available**, **Audio Ports in Use**, and **Video Ports in Use**.

View Bridge Meeting Rooms

To view information about meeting rooms on a bridge

- 1 Go to **Network Device > MCUs**.
- 2 As needed, use the **Filter** to customize the MCU list.
- 3 In the MCU list, select the bridge of interest and click **View Meeting Rooms**.

A **Meeting Rooms** pane appears below the bridge list. It lists the meeting rooms for the selected bridge and identifies the meeting room by **Name**, **ID**, **Duration**, **Conference**, **Chairperson**, **Profile**.

View Bridge Entry Queues

To view information about entry queues on a bridge

- 1 Go to **Network Device > MCUs**.
- 2 As needed, use the **Filter** to customize the MCU list.
- 3 In the MCU list, select the bridge of interest and click **View Entry Queues**.

An **Entry Queues** pane appears below the bridge list. It lists the entry queues for the selected bridge and identifies the entry queue by **Name**, **ID**, **Profile**, and **Dial-In Number**.

View Bridge Gateway Conferences

To view information about gateway conferences on a bridge

- 1 Go to **Network Device > MCUs**.
- 2 As needed, use the **Filter** to customize the MCU list.

- 3** In the MCU list, select the bridge of interest and click **View Gateway Conferences**.

If the feature is available on the bridge, a Gateway Conferences pane appears below the bridge list. It lists the gateway conferences for the selected bridge.

Management Operations for Other Network Devices

This chapter describes how to perform the Polycom® Converged Management Application™ (CMA®) system network device management tasks. It includes:

- [Polycom VBP Management Operations](#)
- [Polycom DMA Management Operations](#)

Polycom VBP Management Operations

The Polycom Video Border Proxy (VBP) device management operations include these topics:

- [Add a Polycom VBP Device](#)
- [Edit a Polycom VBP Device](#)
- [Delete a Polycom VBP Device](#)
- [Identify Endpoints Using the Polycom VBP Device](#)
- [Identify Endpoints Using the Polycom VBP Device](#)

Add a Polycom VBP Device



IMPORTANT

When you add a new Polycom VBP device, the CMA system will restart the user interface web service. This will interrupt others using the CMA system user interface.

To add a Polycom VBP device to a CMA system

- 1 Go to **Network Device > VBPs** and click **Add**
- 2 Configure these settings in the **Add VBP** dialog box.

Column	Description
Name	A unique name to identify the Polycom VBP device.
Provider-side IP	The Private Network IP address for the Polycom VBP device.
Subscriber-side IP	The Public Network IP address for the Polycom VBP device.

- 3 Click **OK**.

A system dialog box appears indicating that you must restart Apache for the settings to take affect. You also have the opportunity to add another Polycom VBP device.

- 4 Click **Restart Apache**.

The Polycom VBP device is added to the CMA system. However, more configuration may be necessary for the device to operate in your network. For example, you will probably need to [“Copy the CMA System Certificate to a Polycom VBP Device”](#) as described in the next topic.

Copy the CMA System Certificate to a Polycom VBP Device

To copy the CMA system certificate to a Polycom VBP device


- 1 Go to **Network Device > VBPs**
- 2 Select the Polycom VBP device of interest and click **Copy Certificate to VBP**.

In the **Copy Certificate to VBP** dialog box, the system automatically populates the **Filename** field with the filename of the CMA system certificate and the **Username** field with root.

- 3 Enter the SSH or console **Password** for the root user and click **OK**.
The Polycom VBP device appears in the **Network Device** list.


Edit a Polycom VBP Device

To edit a Polycom VBP device

- 1 Go to **Network Device > VBPs**
- 2 Select the Polycom VBP device of interest and click **Edit** .
- 3 Configure these settings as needed in the **Edit VBP** dialog box.
- 4 Click **OK**.

Delete a Polycom VBP Device

To delete a Polycom VBP device from a CMA system

- 1 Go to **Network Device > VBPs**.
- 2 Select the Polycom VBP device of interest and click **Delete** .
- 3 Click **Yes** to confirm the deletion.

Identify Endpoints Using the Polycom VBP Device



Note

This procedure identifies only Polycom HDX, Polycom RealPresence Group Series, and CMA Desktop systems that are:

- Registered to the CMA system
- Using the Polycom VBP firewall
- Operating in dynamic-management mode.

One Polycom HDX or legacy endpoint system operating in standard management mode, registered to the CMA system, and using the Polycom VBP firewall may also be displayed in the **Endpoint** list. This entry may represent multiple endpoints, since all Polycom HDX or legacy endpoint system operating in standard management mode register with the same information.

To identify which endpoints are using the Polycom VBP firewall

- 1 Go to **Endpoint > Monitor View**.
- 2 Click **Select Filter** and select **IP Address**.

- 3 Enter the provider-side IP address of the Polycom VBP device and press **Enter**.

The **Endpoint** list displays the dynamically-managed endpoints that are registered to the CMA system and using the Polycom VBP firewall. All of the endpoints display the same IP address, which is the Provider-side IP address of the Polycom VBP device. However, the endpoints will have different aliases and owners.

Polycom DMA Management Operations

The Polycom DMA device management operations includes these topics:

- [Add a Polycom DMA System](#)
- [Edit a Polycom DMA System](#)
- [Delete a Polycom DMA System](#)


Add a Polycom DMA System



IMPORTANT

Newer versions of the DMA system (v3.0 or greater) should not be added to the CMA system in this way. They include call server functionality (H.323 gatekeeper and SIP proxy/registrar), so they do not register with the CMA system as a Gateway/MCU. Instead, these DMA system should be added to the CMA system as a trusted neighbor.


To add DMA system

- 1 Go to **Network Device > DMAs** and click **Add** .
- 2 In the **Add DMA** dialog box, enter a unique and identifying **Name** and **Description** for the DMA system.
- 3 Enter the E.164 dial string prefix for calling the system.
- 4 Click **Add**.

The DMA system appears in the **Network Device** list.

Edit a Polycom DMA System


To edit a DMA system

- 1 Go to **Network Device > DMAs**.
- 2 Select the DMA system of interest and click **Edit** .

- 3 In the **Edit DMA** dialog box, edit the **Name**, **Description** or **Dial Prefix** for the DMA system.
- 4 Click **OK**.

Delete a Polycom DMA System

To delete a DMA system from a CMA system

- 1 Go to **Network Device > DMAs**.
- 2 Select the DMA system of interest and click **Delete** .
- 3 Click **Yes** to confirm the deletion.

View Registered DMA Nodes

Logically, the Polycom DMA system is a cooperative two-node cluster. When the CMA system is the gatekeeper for a DMA system (v2.3 and earlier) both nodes register with the CMA system and can accept and process calls.

The CMA system routes calls destined for the Polycom DMA system to the first node that it finds available. If the first node isn't available, it automatically routes the call to the second node.

To view the registered DMA nodes

- 1 Go to **Network Device > DMAs**.
- 2 Click **View DMA Nodes**.

The DMA Node List appears on the DMA page. It includes these columns

Field	Description
Name	The name of the DMA system node as sent at registration.
IP Address	The IP address of the DMA system node as sent at registration.
Serial Number	The serial number of the DMA system node as sent at registration.
Site	The location of the DMA system node as sent at registration.
Gatekeeper Status	The status of the DMA system node.

MCU Bridge Device Details

This chapter lists the fields found in the MCU Device Detail section of the Polycom® Converged Management Application™ (CMA®) system interface. It includes:

- [MCU H.320 Services](#)
- [MCU H.323 Services](#)
- [MCU Gateway Services](#)
- [MCU Resources—Polycom MGC Platform](#)
- [MCU Resources—Polycom RMX Platform](#)

MCU H.320 Services

Field	Description
MCU H.320 Service	
Service Name	Name of the H.320 ISDN service
Channels	Number of 64K channels dedicated to the MCU
Number Range	Dial-in number range of service. These ISDN numbers are available on an MCU for all endpoints to use. Also called direct inward dialing (DID).
LCR Table	The least-cost routing table for calls made through this gateway
Local Prefix	The prefix required to place a call to a local number outside the enterprise. For example, if you dial 9 to reach an outside line, the Local Prefix is 9.
Non-Local Prefix	The prefix required to dial long distance. For example, in certain states in the United States, you must dial 1 before you can dial a non-local number.

Field	Description
International Prefix	The prefix required to dial an international number. For example, in many countries, the international prefix is 00.
Local Area Code	A list of local area codes, separated by commas
Priority	The priority order for this service

MCU H.323 Services

Field	Description
Service Name	The name of the H.323 service (ASCII only) defined in the MCU.
Dialing Prefix	Prefix to select this service. The prefix for the MGC is located in the H.323 Service Properties dialog box of the MGC Manager.
Service IP Address	IP address associated with this network service and with this H.323 card in the MCU.
Alias	Alias for the service defined in the MCU. Note Polycom recommends using E.164 as the alias for this service. The number is dialed if the endpoints are registered with the same gatekeeper. If the endpoints are not registered with the same gatekeeper, they use their assigned IP address to connect.
Port	Number of IP connections available.
Priority	The priority order for this service.

MCU Gateway Services

Field	Description
Service Name	The name of the H.323 service defined in the MCU.
Dialing Prefix	Prefix to select this service. The prefix for the MGC is located in the H.323 Service Properties dialog box of the MGC Manager.
H320 Service Name	Select a defined H320 service.
Channels	Number of 64K channels dedicated to the MCU.
Priority	The priority order for this service.

MCU Resources—Polycom MGC Platform

Field	Description
Max Total Conferences	Maximum number of total conferences allowed at once on this MCU.
Max CP Conferences	Maximum number of continuous presence (CP) conferences allowed, based on the number of licenses available.
Max Total Participants	Maximum number of total MCU participants allowed at once on this MCU.
Max Transcoding Ports	Maximum number of transcoding ports on which both ISDN and IP participants can be connected.
Total IP Parties (Embedded MCU devices)	Maximum number of IP calls that can be made from this endpoint.
Total ISDN Parties (Embedded MCU devices)	Maximum number of ISDN calls that can be made from this endpoint.
Total Transcoded Parties (Embedded MCU devices)	Maximum number of transcoded calls (IP and ISDN calls combined) that can be made from this endpoint.
Use Entry Queue	Indicates whether the MGC device supports an IVR.
Entry Queue Number ID	The IP number that conference participants dial to access the IVR prompt to join a conference.
Entry Queue ISDN Number	The ISDN-allocated phone number of the IVR. ISDN devices only.

MCU Resources—Polycom RMX Platform

Field	Description
Max Total Conferences	Maximum number of total conferences allowed at once on this MCU.
Max CP Conferences	Maximum number of continuous presence (CP) conferences allowed, based on the number of licenses available.
Max Video Ports	Maximum number of video ports on which participants can be connected.
Max Total Participants	Maximum number of total video participants allowed at once on this MCU.
Use Entry Queue	Indicates whether the RMX device supports an IVR.
Entry Queue Number ID	The number that conference participants dial to access the IVR prompt to join a conference.
Entry Queue ISDN Number	The number that conference participants dial to access the IVR prompt to join a conference.
Audio & Video Settings: The following parameters must be set manually to synchronize with the RMX device. See the RMX documentation for more information about these settings.	
Max Voice Ports	<p>Set this to the maximum number of audio ports configured on the RMX device.</p> <p>Refer to the <i>RMX 2000/4000 Administrator's Guide</i> for more information about this field.</p> <p>Note</p> <p>Up to 10 blocks of RMX video ports can be converted to 50 audio-only ports, up to a maximum of 200 audio-only ports.</p>
Max CP Resolution	<p>Set this to the highest available video format. Choices are: HD1080, CIF, SD15, SD30, and HD720.</p> <p>Refer to the <i>RMX 2000/4000 Administrator's Guide</i> for more information about this field.</p>
Max Bandwidth Capacity (Kbps)	The maximum bandwidth to the Polycom RMX system.

Users and Groups Overview

This chapter provides an overview of the Polycom® Converged Management Application™ (CMA®) system users and groups management structure. It includes these topics:

- [Overview of Groups, Users, and User Roles](#)
- [Roles and Permissions](#)
- [Device Associations and Presence](#)

Overview of Groups, Users, and User Roles

The CMA system allows users assigned the **Administrator** role to manage users, groups, user roles, permissions, and areas (if applicable).

Most often, a CMA system is integrated with an enterprise directory from which users are imported. However, the CMA system also allows administrators to add local users (that is, users added manually to the system) and associate them with endpoints, groups, and roles.

Users

Local Users

When you manually add local users, the CMA system manages all user information and associations.

At a minimum, when you manually add users, you must enter a user's **First Name** or **Last Name**, **User ID**, and **Password**. When you enter the minimum information, the CMA system automatically assigns local users the basic **Scheduler** role, unless you remove that assignment. They can then schedule conferences, be scheduled into conferences, and call into conferences. However, the system cannot call out to them until they are associated with endpoints.

You should associate local users with one or more roles and associate them with one or more endpoints. Alternatively, you can associate local users with roles by associating them with local groups.

If your company has implemented the **Areas** feature, you can also associate local users with areas for which you are an administrator. For more information about areas, see [“Area Overview and Operations”](#) on page 347.

Enterprise Users

When the CMA system is integrated with an enterprise directory, the CMA system manages only the following pieces of an enterprise users’ information: the endpoints, roles, alert profiles, and areas assigned to them. The remaining information is pulled from the enterprise directory.



Notes

- Currently, the CMA system supports only a Microsoft Active Directory implementation of an LDAP directory.
- The CMA system displays a user’s **City**, **Title**, and **Department** to help distinguish between users with the same name.

When the CMA system is integrated with an enterprise directory, users imported into the system through the enterprise directory are by default added to the system without a role. This default set up allows users to log into the CMA system with their enterprise user IDs and passwords. They can then be scheduled into conferences and call into conferences. However, the system cannot call out to them until they are associated with endpoints.

To be fully functional, you must associate enterprise users with one or more roles to control their access to system functions and associate them with one or more endpoints. Alternatively, you can associate enterprise users with roles by associating them with local or enterprise groups.

If your company has implemented the Areas feature, you can also associate enterprise users with areas for which you are an administrator. For more information about areas, see [“Area Overview and Operations”](#) on page 347.

If you want the CMA system to, by default, automatically assign enterprise users the basic **Scheduler** role, you must change the appropriate system **Security Settings**. See [“Give Enterprise Users Default Scheduler Role”](#) on page 455.

Groups

Groups provide a more efficient and consistent use of the CMA system, because they allow you to assign roles and provisioning profiles to sets of users rather than to individual users.

Local Groups

The CMA system allows you to add local groups (that is, groups added manually to the system) and associate them with provisioning profiles and roles.

For local groups, the CMA system manages all group information and associations.

Enterprise Groups

When the CMA system is integrated with an enterprise directory, groups defined to the enterprise directory are not automatically added to the CMA system, but you can import them into the system.

When the CMA system is integrated with an enterprise directory, the system manages only three pieces of group information: the provisioning profile assigned to the group, the roles assigned to the group, and whether or not the group is Directory Viewable (that is, displayed in endpoint directories). The remaining group information is pulled from the enterprise directory.

To take full advantage of the CMA system, the enterprise Microsoft Active Directory must:

- Have Global Catalog turned ON. The Global Catalog enables searching for Active Directory objects in any domain without the need for subordinate referrals, and users can find objects of interest quickly without having to know what domain holds the object.
- Use universal groups. The Global Catalog stores the member attributes of universal groups only. It does not store local or global group attributes.
- Have a login account that has read access to all domains in the Active Directory that the CMA system can use. We recommend an account with an administrative username and a non-expiring password.
- Have the Active Directory Domain Name Service correctly configured. For more information about Active Directory design and deployment, see the Microsoft best practices guides at <http://technet.microsoft.com>.

For system and endpoint directory performance purposes, two best practices in regards to enterprise groups are:

- Do not import more than 500 enterprise groups into a CMA system.
- Do not mark more than 200 enterprise groups as **Directory Viewable**.

Roles and Permissions

The CMA system is a role and permissions based system.

- Users are assigned one or more user roles either directly or through their group associations.
- User roles are assigned a set of permissions.
- Users see only the pages and functions available to their roles and associated permissions. Permissions are cumulative, so users see all of the pages and functions assigned to all of their roles and associated permissions.



Notes

- Users inherit roles from their parent groups—local or enterprise. They cannot inherit roles from groups more distantly removed—for example, from their grandparent groups.
- The role names **Administrator**, **Operator**, and **Scheduler** are stored in the system database and are not localized into other languages. If you wish to localize their names into your language, edit the roles and enter new names for them.

- If your company has implemented the Areas feature, users only see endpoints assigned to their areas.

An administrator has several options when implementing user roles.

- 1 Implement only the default user roles and keep the standard permissions assigned to these roles.
- 2 Implement only the default user roles but change the permissions assigned to these roles.



Note

To ensure CMA system access and stability, the default Administrator role cannot be deleted or edited.

- 3 Implement either option 1 or 2, but also create additional unique, workflow-driven user roles and determine which permissions to assign to those user roles.

While the CMA system allows businesses almost unlimited flexibility in defining roles, for simplicity and clarity, we recommend keeping the default roles with their default permissions and responsibilities. Because users can be assigned multiple roles, and permissions are cumulative, your business can combine roles as needed to reflect the workload your people undertake to manage and use the system.

Some important notes about user roles and permissions:

- Users (local and enterprise) may be assigned more than one role. In this case, the permissions associated with those roles are cumulative; a user has all of the permissions assigned to all of his roles.
- Users (local and enterprise) may be assigned roles as an individual and as part of a group. Again, the permissions associated with those roles are cumulative; a user has all of the permissions assigned to all of his roles no matter how that role is assigned.
- Users assigned a role with any one of the **Administrator Permissions** are generally referred to as administrators. Users assigned a role with any one of the **Operator Permissions** and none of the **Administrator Permissions** are referred to as **Operators**. Users assigned a user role with **Scheduler Permissions** and none of the **Administrator** or **Operator Permissions** are referred to as **Schedulers**.

Default CMA System Roles and Permissions

The CMA system includes a default set of roles. Roles are associated with a set of permissions. Roles and permissions define the menus, pages, and functions that the system displays. So users see only the menus, pages, and functions associated with their roles.

The following table identifies the default roles. Each of these roles is discussed in more detail in the following sections.



Note

The role names are stored in the system database and are not localized into other languages. If you wish to localized the role names into your language, edit the roles and enter new names for them.

Role	Permissions	Comment
Scheduler	Schedule Conferences Scheduling Level = Basic	
Advanced Scheduler	Schedule Conferences Scheduling Level = Advanced	
View-Only Scheduler	Schedule Conferences Scheduling Level = View-Only	Users with this role cannot schedule conferences; they can only see conferences scheduled
Operator	Conference Operator Reports Troubleshooting	

Role	Permissions	Comment
Device Administrator	Monitoring	
Administrator	Directory Setup Dial Plan Setup Conferencing Setup System Setup Assign Users to Areas (when activated) Associate Devices to Areas (when activated) System Maintenance/Troubleshooting Provision Profiles	This role cannot be deleted or edited.
Auditor	Auditor	

Except when operating in maximum security mode, most users will also see these menu items:

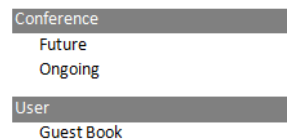
Description
<p>Settings. Click here to display a Settings dialog box with the following information:</p> <ul style="list-style-type: none"> • User Name • Remote Server • Software Version • Font Size <p>In this dialog box, you can also:</p> <ul style="list-style-type: none"> • Change the font size used in your display of the CMA system web client interface. • Change your password, if you are a local system user.
<p>Downloads. Click here to display the Downloads dialog box with the downloadable applications that are compatible with the CMA system. Downloadable applications include:</p> <ul style="list-style-type: none"> • CMA Desktop client for PC or MAC (including the path to the application) • Polycom Scheduling Plugin for Microsoft Outlook • Polycom Scheduling Plugin for IBM Lotus Notes • Polycom File Verification Utility
<p>Log Out. Click here to log out of the CMA system.</p> <p>Note</p> <p>The CMA system has an inactivity timer. If you are logged into the system but do not use the interface for a specified period of time (10 minutes by default), the system automatically logs you out.</p>
<p>Help. Links to the CMA system online help.</p>

Scheduler Roles, Responsibilities, and Menus

The CMA system offers three different default **Scheduler** roles.

Role	Responsibilities
Scheduler	For the areas to which they belong (areas are optional), users assigned the Scheduler (sometimes called basic scheduler) role can schedule conferences. They do so using the conference templates defined for them. But basic schedulers cannot change any of the conference settings defined in the templates they choose when scheduling their conferences.
Advanced Scheduler	For the areas to which they belong (areas are optional), users assigned the Advanced Scheduler role can also schedule conferences. And again they do so using the conference templates defined for them. But advanced schedulers can change selected conference settings defined in the template they use when scheduling their conferences.
View-Only Scheduler	For the areas to which they belong (areas are optional), users assigned the View-only Scheduler role cannot schedule conferences; they can only see conferences that have been scheduled.

When basic or advanced schedulers log into the CMA system, the system displays the **Future** conference page and they have access to the following menu items:



When view-only schedulers log into the CMA system, the system displays the **Ongoing** conference page and it is the only menu item to which they have access.

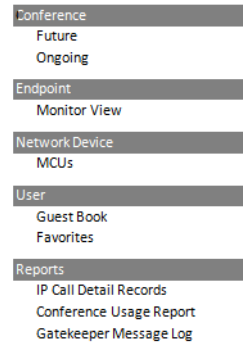
Operator Role, Responsibilities, and Menus

The **Operator** role allows businesses to offer high-touch customer service for video conferencing. For the areas to which they belong, users assigned the **Operator** role can:

- Schedule conferences.
- Monitor and manage ongoing conferences.
- Monitor endpoints.

- Monitor network devices such as MCUs.
- Add, edit, and delete entries in the system **Guest Book**.
- Create favorites.
- View some system reports.

When operators log into the CMA system, the system displays the **Ongoing** conference page and they have access to the following menu items:

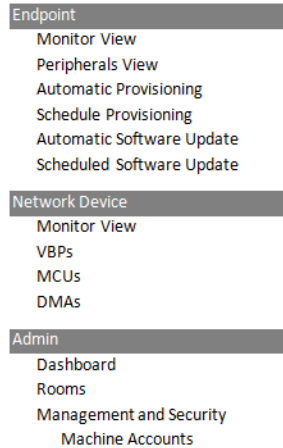


Device Administrator Role, Responsibilities, and Menus

The **Device Administrator** role is for those users who administrate endpoints, bridges, and other network devices. For the areas to which they belong, users assigned the **Device Administrator** role can:

- Monitor endpoints, peripherals, and network devices.
- Add, edit, and delete endpoints and network devices.
- Provision endpoints.
- Update endpoints.
- Add, edit, and delete rooms.

When device administrators log into the CMA system, the system displays the system **Dashboard** and they have access to the following menu items:



Auditor Role, Responsibilities, and Menus

The **Auditor** role allows security-conscious companies to separate system administration functions from system auditing functions. This provides an added level of system checks and balances. This role must be explicitly assigned by an administrator.

For the areas to which they belong, users assigned the **Auditor** role can:

- View audit logs.
- Backup and delete audit logs.
- Change the audit log file alert level.
- Generate online Endpoint Usage Reports.
- Download CDRs.
- View and download system log files.
- Download Windows event logs.
- Respond to audit log alerts.

When auditors log into the CMA system, the system displays the **Audit Log Files** page and they have access to the following menu items:



Administrator Role, Responsibilities, and Menus

The **Administrator** role is for those users who administrate the CMA system itself. Users assigned the **Administrator** role can generally do almost all system functions, however they cannot schedule conferences, monitor conferences, or manage endpoints or other network devices.

When administrators log into the CMA system, the system displays the system **Dashboard** and they have access to the following menu items:

Endpoint	Admin	Admin (continued)
Monitor View	Dashboard	Gatekeeper Settings
Peripherals View	Conference Templates	Primary Gatekeeper
	Conference Settings	Alternate Gatekeeper
Network Device	Provisioning Profiles	Neighboring Gatekeepers
Monitor View	Automatic Provisioning Profiles	Management and Security
MCUs	Scheduled Provisioning Profiles	Server Software Upgrade
User	Software Updates	Certificate Settings
Users	Automatic Software Updates	Security Settings
Groups	Scheduled Software Updates	Endpoint Management Settings
User Roles	Rooms	Dial Plan and Sites
Guest Book	Areas	Site Topology
Reports	Directories	Sites
Site Statistics	Address Books	Site-Links
Site-Link Statistics	Global Address Book	Site-to-Site Exclusions
IP Call Detail Records	Enterprise Directory	Network Clouds
Endpoint Usage Report	Directory Setup	Territories
Conference Usage Report	Server Settings	Services
Conference Type Report	Network	Dial Rules
Gatekeeper Message Log	System Time	LCR Tables
System Log Files	Database	Alert Settings
Audit Log Files	Calendar Management	CMA Alert Level Settings
	Microsoft Lync Integration	Endpoint Alert Level Settings
	Licenses	Remote Alert Profiles
	Redundant Configuration	Database Backup Files
	Custom Logo	Troubleshooting Utilities
	Remote Alert Setup	Report Administration
	E-mail	
	SNMP Settings	

Customized Roles and Responsibilities

The CMA system allows you almost unlimited flexibility in defining and redefining roles, but for simplicity and clarity, we recommend keeping the default roles with their default permissions and responsibilities.

Users can be assigned multiple roles and permissions are cumulative, so your business can combine roles as needed to reflect the workload your people undertake to manage and use the system.

Device Associations and Presence

The CMA system assumes that users will be associated with endpoints. You can associate a user with more than one endpoint, but one endpoint is designated as the primary endpoint.

When scheduling a user in a conference, the CMA system will, by default, schedule the user's primary endpoint. The scheduler can choose to change the request to schedule one of the user's other endpoints.

The CMA system is also a presence service, which is the part of the system that maintains online status information for the users of dynamically managed endpoints. The presence service allows users to access information about the online status of other users. This is important, because when you make a video call or start a chat, that action only takes you to an endpoint. It doesn't ensure that you will reach the person you want to reach. The presence service provides information about the user's availability, which improves your chances of getting the person.

User Management Operations

This chapter includes information on managing users and groups within the Polycom® Converged Management Application™ (CMA®) system. It includes these topics:

- [Manage Users](#)
- [Manage Groups](#)
- [Manage User Roles](#)
- [Manage System Guest Book](#)
- [Manage Favorites](#)

Manage Users

In the CMA system, only users assigned the **Administrator** role can manage a user. Some of these tasks include:

- [Search for a User](#)
- [Add a Local User](#)
- [Edit a User](#)
- [View Permissions for a User](#)
- [Delete a User](#)

Search for a User

To search for a user

- 1 Go to **User > Users** and in the **Search Users** field, enter the name of the user of interest.

**Note**

Searches for a user are case-insensitive, prefix searches of the **Username**, **First Name**, and **Last Name** fields.

- 2 To search for a local user, press **Enter**.
- 3 To search both local and enterprise users, first clear the **Local Users Only** check box and then press **Enter**.

**Note**

If you are not in an enterprise domain, you will not have the option of searching for enterprise users.

The first 500 users in the database that match your search criteria are displayed in the **Users** list.

- 4 If the list is too large to scan, further refine your search string.

View User Information

You can view information about a user, local or enterprise.

To view the address book a user is assigned to

- 1 Go to **User > Users**.
- 2 Select the user you want.
- 3 Click **View Details**.

Column	Description
General Info	
First Name	The user's first name.
Last Name	The user's last name.
User ID	The user's unique login name. This user ID must be unique across all rooms and users and across all domains.
Email Address	<p>The user's E-mail address. (The E-mail address is an ASCII-only field.)</p> <p>Note</p> <p>The CMA system identifies plugin users and their associated endpoints by E-mail address, so this is required information for the plugin to work.</p>

Column	Description
Title	The user's professional title.
Department	The user's department within the enterprise.
City	The city in which the user's office is located.
Phone Number	The contact phone number for the user.
Associated Permissions	
Permission	The set of permissions the user is assigned. For more information, see "Roles and Permissions" on page 252.
Granted Through	The role through which the permissions are assigned.
Associated Roles	
Assigned Roles	The roles assigned to the user. For more information, see "Roles and Permissions" on page 252.
Groups	
Type	The type of group to which the user belongs. Possible values are local and enterprise.
Name	The name of the group to which the user belongs.
Inherited Group Info	
Address Book	The Address Book(s) the user sees based upon the groups to which the user is assigned.

Add a Local User

To add a local user

- 1 Go to **User > Users** and click **Add**.

The **Add New User** dialog box appears. The **Enable User** option is selected by default.

- 2 Enter the following user information.

Column	Description
First Name	The user's first name
Last Name	The user's last name

Column	Description
User ID	The user's unique login name. This user ID must be unique across all rooms and users and across all domains.
Password	The user's assigned password. This password must be a minimum of eight characters in length.
Email Address	<p>The user's E-mail address. (The E-mail address is an ASCII-only field.)</p> <p>Note</p> <p>The CMA system identifies plugin users and their associated endpoints by E-mail address, so this is required information for the plugin to work.</p>
Title	The user's professional title
Department	The user's department within the enterprise
City	The city in which the user's office is located
Phone Number	The contact phone number for the user

- 3 In the **Associated Endpoints** section, select and move the required endpoints(s) to **Selected Endpoints** list. Move the unwanted endpoints(s) to the **Available Endpoints** list. Press **Shift-click** or **Ctrl-click** to select multiple items in the list.
- 4 In the **Associated Roles** section, select and move the required role(s) to **Selected Roles** list. Move the unwanted role(s) to the **Available Roles** list. Press **Shift-click** or **Ctrl-click** to select multiple items in the list.



Note

If the user has multiple endpoints, list the endpoints in order of priority, with the primary endpoint first.

- 5 If Areas are enabled, in the **Associated Areas** section, select one of the following options to associate the user with an area.
 - **None** – Does not allow access to any endpoints.
 - **All Areas** – Gives the user access to all endpoints, regardless of the area the endpoints are assigned to.
 - **Specific Areas** – Give the user access to only endpoints assigned to the areas selected below. Select one or more areas in the list below and click the right arrow.
- 6 In the **Associated Alert Profile** section, select a **Remote Alert Notification Profile** as appropriate.

- 7 In the **Dial String Reservations** section, select the user's **endpoint** and enter the appropriate dial strings for **SIP URI**, **E164**, and **H323 ID**, then click **Apply**.

The dial strings appear in the list below.

If the user has multiple endpoints, enter the dial strings for one endpoint type at a time and click **Apply** each time.

- 8 Click **OK**.

If the **Phone Number** you entered is exactly the same as an existing user or endpoint, the **Phone Number Conflict** dialog box appears and lists the names of the other users or endpoints with the same number.

- To keep the duplicate number, click **Continue**.
- To change the phone number, click **Cancel**.

Edit a User

For local users added manually to the CMA system, you can edit all user information. If you change the user ID, the user must log into the associated endpoints with the new ID.

For users added through the enterprise directory, you can edit their roles (unless the role is inherited from a group) and associate them to endpoints, but you cannot change user names, user IDs, or passwords.

To edit a user

- 1 Go to **User > Users** and in the **Search Users** field, enter the name of the user of interest.



Note

Searches for a user are case-insensitive, prefix searches of the **Username**, **First Name**, and **Last Name** fields.

- 2 To search for a local user, press **Enter**.
- 3 To search both local and enterprise users, first clear the **Local Users Only** check box and then press **Enter**.



Note

If you are not in an enterprise domain, you will not have the option of searching for enterprise users.

- 4 If the list is too large to scan, further refine your search string.
- 5 Select the user of interest and click **Edit**.

- 6 As required, edit the **General Info**, **Associated Devices**, **Associated Roles**, **Associated Areas**, **Associated Alert Profile**, and **Dial String Reservations** sections of the **Edit User** dialog box.
- 7 Click **OK**.

View Permissions for a User

A user with the **Administrator** role can view permissions for a user.

To view permissions for a user

- 1 Go to **User > Users** and in the **Search Users** field, enter the name of the user of interest.



Note

Searches for a user are case-insensitive, prefix searches of the **Username**, **First Name**, and **Last Name** fields.

- 2 To search for a local user, press **Enter**.
- 3 To search both local and enterprise users, first clear the **Local Users Only** check box and then press **Enter**.



Note

If you are not in an enterprise domain, you will not have the option of searching for enterprise users.

- 4 If the list is too large to scan, further refine your search string.
- 5 Select the user of interest and click **View Permissions**.
The **View Permissions** dialog box displays the permissions information.
 - **Permission**—Lists the permissions assigned to the user.
 - **Granted Through**—Role assigned to the user that grants the listed permissions.
- 6 Click **Close**.

Delete a User

You can only delete local users from the CMA system. You cannot delete users added through integration with an enterprise directory.

To delete a user

- 1 Go to **User > Users** and in the **Search Users** field, enter the name of the user of interest.

**Note**

Searches for a user are case-insensitive, prefix searches of the **Username**, **First Name**, and **Last Name** fields.

- 2 To search for a local user, press **Enter**.
- 3 To search both local and enterprise users, first clear the **Local Users Only** check box and then press **Enter**.

**Note**

If you are not in an enterprise domain, you will not have the option of searching for enterprise users.

- 4 If the list is too large to scan, further refine your search string.
- 5 Select the user of interest and click **Delete**.
- 6 Click **Yes** to confirm the deletion.

The user is deleted from the CMA system.

Unlock a User Account

When a local user reaches the **Failed login threshold**, the system will not allow the user to log in until an administrator unlocks the user's account. When a user's account is locked, the system will display an error message.

To unlock a user account

- 1 Go to **User > Users** and in the **Search Users** field, enter the name of the user of interest and press **Enter**.
- 2 Select the user of interest and click **Edit**.
- 3 Enable the **Unlock User** option and click **OK**.

The system should allow the user to log in.

Manage Groups

In the CMA system, only users assigned the **Administrator** role can:

- [Add a Local Group](#)
- [Import Enterprise Groups](#)
- [Edit a Group](#)
- [Delete a Group](#)

Add a Local Group

To add a local group

- 1 Go to **User > Groups**.
- 2 In the **Groups** page, click **Add Local Group**.
- 3 Complete the **General Info** section of the **Add Local Group** dialog box.

Column	Description
General Info	
Group Name	A meaningful and unique group name assigned when creating the group.
Description	A more complete description of the group's purpose
Directory Viewable	Whether or not the group is displayed in the endpoint directory
Provisioning Profile	The automatic provisioning profile assigned when creating the group
Address Book	See "Assign Address Books to Groups" on page 379.
Associated Roles	
Available Roles	The list of roles defined to the CMA system
Selected Roles	The list of roles that you assign users when adding them to the system. Users have all of the permissions associated with all of the roles assigned to them (that is, permissions are cumulative).

Column	Description
Group Members (Local Users Only)	
Search Available Members	Search field for finding users
Search Results	The users and groups identified to the system that you can add to the local group. This list can include both local and enterprise users and groups.
Group Members	The users and groups selected as part of the group

- 4 In the **Search Available Members** field of the **Group Members** dialog box, search for the users and groups to add to this local group.
- 5 In the **Search Results** section, select and move the users and groups of interest to the **Group Members** list. To select all users and groups listed, click the check box in the column header.
- 6 Click **OK**.

The group appears in the **Groups** list. It is identified as a LOCAL group.

Import Enterprise Groups

To import one or more enterprise groups

- 1 Go to **User > Groups**.
- 2 In the **Groups** page, click **Import Enterprise Group**.
- 3 In the **Search Available Groups** field of the **Import Enterprise Group** dialog box, type all or part of the group name (with wildcards) and press **ENTER**.



Note

Searches for a group are case-insensitive, exact-match searches of the **Group Name** field. Use wildcard characters to perform substring searches.

- 4 In the **Search Results** list, select the enterprise groups to add. To select all enterprise groups, click the check box in the column header.
- 5 Click the right arrow to add the enterprise groups to the **Groups to Import** list.
- 6 Click **OK**.

The enterprise group appears in the **Groups** list. Now you can edit the group and associate it with an automatic provisioning profile, user roles, and specify whether or not the group directory is viewable. You can also search for enterprise users.

Edit a Group

To edit a local or enterprise group

- 1 Go to **User > Groups**.
- 2 In the **Groups** page, select the group of interest and click **Edit**.
- 3 As required, edit the **General Info**, **Associated Roles**, and **Group Members** sections of the **Edit Local Groups** dialog box.



Notes

- The **Group Members** section is only available for Local groups.
- If you remove a user from a group or a role from a group, the user no longer has the roles associated with the group.

- 4 Click **OK**.

Delete a Group

To delete a local or enterprise group

- 1 Go to **User > Groups**.
- 2 In the **Groups** page, select the group of interest and click **Delete Group**.
- 3 Click **Yes** to confirm the deletion.

The group is deleted from the CMA system.



Note

An enterprise group is only deleted from the CMA system, not the enterprise directory, so it can be reimported.

Manage User Roles

In the CMA system, only users assigned the **Administrator** role can:

- [Assign Users Roles and Endpoints](#)
- [View the List of User Roles](#)
- [Add a User Role](#)
- [Edit Permissions for a User Role](#)
- [Delete a User Role](#)

- [View the Groups and Users Associated with a User Role](#)

Assign Users Roles and Endpoints

You can assign roles to both local and enterprise users and associate them with endpoints.

To assign a role and endpoint to a user

- 1 Go to **User > Users**.
- 2 To search for a user:
 - a In the **Search** field of the **Users** page, type a search string.



Note

Searches for a user on the CMA system **Users** page are case-insensitive, prefix searches of the **Username**, **First Name**, and **Last Name** fields.

- b To search both local and enterprise users, clear the **Local Users Only** check box and press **Enter**.

The first 500 users in the database that match your search criteria are displayed in the **Users** list.
 - c If the list is too large to scan, further refine your search string.
- 3 Select the user of interest and click **Edit**.
- 4 In the **Devices** section of the **Edit User** dialog box, select the endpoint to associate with the user and move it to the **Selected Devices** column. If a user has multiple endpoints, the first endpoint listed is the user's default endpoint.
- 5 Click **Finish**.

View the List of User Roles

To view the list of User Roles

- Go to **User > User Roles**.

The **User Roles** list appears. It can be filtered by **Name** and **Description**.

Column	Description
Name	The unique name of the user role
Description	An optional description of the role

Add a User Role

When you add a user role, you also specify permissions for the role.

To add a new user role

- 1 Go to **User > User Roles**.
- 2 On the **User Roles** page, click **Add**.
- 3 Complete the **Name** and **Description** fields of the **Add Role** dialog box and assign permissions to the new role.

The following table describes the fields of the **Add Role** dialog box.

Field	Description
Name	The unique name (ASCII only) of the user role
Description	(Optional) A useful description (ASCII only) of the user role
Administrator Permissions	Identifies which CMA system administrator pages and functions are available to the user role.
Operator Permissions	Identifies which CMA system operator pages and functions are available to the user role.
Scheduler Permissions	<p>Identifies which CMA system scheduling pages and functions are available to the user role.</p> <p>Scheduling Level. This setting determines the level of scheduling available through this role. Possible values are:</p> <ul style="list-style-type: none"> • Basic. Users can schedule conferences using the conference templates defined for them. They cannot access or edit the advanced Conference Settings. • Advanced. Users can schedule conferences using the conference templates defined for them. They can also access and edit the advanced Conference Settings.

- 4 Click **Save**.

The new user role appears in the CMA system.

Edit Permissions for a User Role

You can change permissions for the default **Operator** and **Scheduler** roles, as well as for other user roles that were created manually. You cannot change permissions for the default **Administrator** role.

To edit the permissions for a user role

- 1 Go to **User > User Roles**.

- 2 As needed, use the **Filter** to customize the **User Roles** list.
- 3 In the **User Roles** list, select the role of interest and click **Edit**.
- 4 Edit the **Description** field of the **Edit Role** dialog box and edit permissions for the role.
- 5 Click **Save**.

Delete a User Role

You can delete a user role from the CMA system, provided no users are currently assigned to it.

To delete a user role

- 1 Go to **User > User Roles**.
- 2 As needed, use the **Filter** to customize the **User Roles** list.
- 3 In the **User Roles** list, select the role of interest and click **Delete**.
- 4 Click **Yes** to confirm the deletion.

The user role is deleted from the CMA system.

View the Groups and Users Associated with a User Role

To view which groups and users are associated with a specific user role

- 1 Go to **User > User Roles**.
- 2 As needed, use the **Filter** to customize the **User Roles** list.
- 3 In the **User Roles** list, select the role of interest and click **View Associated Groups and Users**.

The **View Associated Groups and Users** dialog box appears.

Manage System Guest Book

This section includes some general information you should know about the Conference menu and views. It includes these topics:

- [User Menu and Guest Book](#)
- [Context-Sensitive Guest Book Actions](#)
- [Add a Guest to the System Guest Book](#)
- [Edit a Guest in the System Guest Book](#)
- [Delete a Guest from the System Guest Book](#)

User Menu and Guest Book

By default, schedulers, operator, and administrators have access to the **User Menu** and **Guest Book**.

The **Guest Book** is a local system directory that includes guest participants who were either:

- Explicitly added to the **Guest Book**.
- Saved to the **Guest Book** while being added as conference participants.

They are referred to as static entries because they are not imported through the dynamically updated enterprise directory or included in the system **Global Address Book**. The **Guest Book** is limited to 500 entries. The **Guest Book** has these fields.

Field	Description
Name	The guest's first and last name.
Email	The guest's E-mail address. The system validates the E-mail structure only.
Location	The location of the guest's endpoint system. This is a free-form entry field that the system does not validate.
Number	(Optional) The ISDN phone number for the user. This number is constructed from the Country code + Area/City code + phone number or entered as the modified dial number.
Join Mode	Indicates whether the guest will use an audio endpoint or video endpoint to join conferences.
Dial Options	Indicates whether the guest will dial into conferences or that the system should dial out to the guest.
Dial Type	Indicates whether the guest has an H.323 (IP), SIP (IP), or H.320 (ISDN) endpoint.

Context-Sensitive Guest Book Actions

The **Actions** section of the **Guest Book** page may include these context-sensitive actions depending on what is selected.

Actions	Description
Add Guest	Use this command to add a new guest user.
Edit Guest	Use this command to change information for a guest user.
Delete Guest	Use this command to delete a guest from the Guest Book . Deleting a guest is a permanent operation.

Add a Guest to the System Guest Book

To add a guest to the system Guest Book

- 1 Go to **User > Guest Book** and click **Add Guest**.
- 2 Configure the **Guest Information** section of the **Add New Guest** dialog box.

Field	Description
First Name	The guest's first name.
Last Name	The guest's last name.
Email	The guest's E-mail address. The system only validates the structure of the E-mail address.
Location	The location of the guest's endpoint system. This is a free-form field that the system does not validate.
Dial Type	Specify the protocol that the guest's endpoint supports: H.323 (IP), SIP (IP), or H.320 (ISDN). This selection will determine what other sections of the Add New Guest dialog box you will need to complete.
Join Mode	Specify whether the guest's endpoint is an audio or video endpoint. Note A guest may have multiple endpoints. Create a separate Guest Book entry for each endpoint.

Field	Description
Dial Options	<p>Specify whether the guest will dial into conferences, or require that the system dial out to the guest.</p> <p>Note</p> <p>To support both options, create a separate Guest Book entry for each.</p>

3 If the guest has an H.323 (IP) endpoint, configure these settings:

Field	Description
Number and Number Type	<p>The specific dial string for the guest, and the format of the number that the MCU must resolve to contact the guest. This may be an IP address, E.164 address, H.323, or Annex-O.</p> <p>For Annex-O dialing, in the Number field enter the <i>H.323.alias@IP</i>, for example:</p> <ul style="list-style-type: none"> • <i>1001@11.12.13.14</i> • <i>1001@domain.com</i> • <i>username@domain.com</i> • <i>username@11.12.13.14</i> <p>Notes</p> <ul style="list-style-type: none"> • Polycom endpoints must register with a gatekeeper before they will attempt an Annex-O call. • You can enter a dial string for another MCU as a guest. If so, you may need to specify the conference ID in the Extension field also.
Extension	<p>Use this field to connect the conference to another conference on another MCU. In this field, specify the conference ID or passcode for the conference on the other MCU.</p>
MCU Service	<p>Choose from the list of MCU services defined on the MCUs with which the CMA system is registered. Leave this at Any Available Service unless you have specific knowledge of MCU services.</p>

4 If the guest has a SIP (IP) endpoint, configure these settings:

Field	Description
Sip URI	The SPI URI the MCU must resolve to contact the guest.
MCU Service	Choose from the list of MCU services defined on the MCUs with which the CMA system is registered. Leave this at Any Available Service unless you have specific knowledge of MCU services.

- 5 If the guest has an H.320 (ISDN) endpoint, configure these settings:

Field	Description
Use Modified Dial Number	Select this option first (as needed) as it will determine the other fields you must configure.
Country	(Not available when Use Modified Dial Number is selected.) The country to which the system will dial out to the guest. Click Select to view a list of country codes.
Area/City Code	(Not available when Use Modified Dial Number is selected.) The area code to which the system will dial out to the guest.
Number	The participant's phone number.
Extension	Cannot be configured.
MCU Service	Choose from the list of MCU services defined on the MCUs with which the CMA system has registered. Leave this at Any Available Service unless you have specific knowledge of MCU services.

- 6 Click OK.

Edit a Guest in the System Guest Book

To edit a guest in the system Guest Book

- 1 Go to **User > Guest Book** and select the guest of interest.
- 2 Click **Edit Guest**.
- 3 Change the **Guest Information** section and endpoint information sections of the **Add New Guest** dialog box, as needed. For more information about these fields, see ["Add a Guest to the System Guest Book"](#) on page 276.
- 4 Click **OK**.

Delete a Guest from the System Guest Book

To delete a guest from the system Guest Book

- 1 Go to **User > Guest Book** and select the guest of interest.
- 2 Click **Delete Guest**.
- 3 Click **Yes** to confirm the deletion.

Manage Favorites

The CMA system allows operators with **Monitoring** permissions to create one or more **Favorites** list, which they can use to quickly select participants to participate in conferences.

The operations associated with managing favorites include:

- [Add a Favorites List](#)
- [Edit a Favorites List](#)
- [Delete a Favorites List](#)

In the CMA system, only operators with **Monitoring** permissions can view, add, edit, delete, or use **Favorites** lists and these **Favorites** lists cannot be shared with other operators.

Add a Favorites List

To add a Favorites list

- 1 Go to **User > Favorites**.
- 2 On the **Favorites** page, click **Add**.
- 3 Complete the **Favorites List Name** and **Description** fields of the **Add Favorites List** dialog box.

Note

The **Favorites List Name** must be unique within the system.

- 4 In the **Search Available Members** field enter all or part of the person's last name or first name and click **Search**.

The system searches the **Users** list (local and domain) for users who are associated with endpoints and who meet your search criteria. The results appear in the **Search Results** column.

Notes

- Depending on the search domain, the search function may return different results. See [Filter and Search a List](#).
- The search results only include users associated with endpoints.

- 5 Select the user(s) of interest from the list and move them to the **Favorite List Members** column.
- 6 Repeat step 4 and 5 until you've added the users of interest to your **Favorites** list and then click **OK**.

The new list appears in the **Favorites** page.

Edit a Favorites List

To edit a Favorites list

- 1 Go to **User > Favorites**.
- 2 On the **Favorites** page, select the **Favorites** list of interest and click **Edit**.
- 3 In the **Edit Favorites List** dialog box, edit the **Favorites List Name** and **Description** fields as needed.
- 4 Remove or add users to the **Favorite List Members** column as needed and then click **OK**.

Delete a Favorites List

To delete a Favorites list

- 1 Go to **User > Favorites**.
- 2 On the **Favorites** page, select the **Favorites** list of interest and click **Delete**.
- 3 Click **Yes** to confirm the deletion.

The list is deleted from the CMA system.

System Reports

This chapter describes the reports available through the Polycom® Converged Management Application™ (CMA®) system and how to view and export them. Use these reports to identify return on investment, troubleshoot problems, provide information about network traffic, and ensure accurate billing for Polycom video calls.

The topics include:

- [Site Statistics Report](#)
- [Site Link Statistics Report](#)
- [H.323 Call Detail Records Report](#)
- [Endpoint Usage Report](#)
- [Conference Type Report](#)
- [Gatekeeper Message Log](#)
- [View and Export System Log Files](#)
- [Download Windows Event Log Files](#)
- [View and Download Audit Log Files](#)
- [CMA System Report](#)

Site Statistics Report

Use the **Site Statistics** report to check call rate and call quality statistics for the sites. You can view the data in a grid or graphically.

To view Site Statistics**1** Go to **Reports > Site Statistics**.

The **Site Statistics** appear with the statistics displayed in a grid. The grid shows a snapshot of the current statistics. The data is updated automatically every 15 seconds.

Column	Description
Site Name	Specifies the site to which the statistics apply.
Num of Calls	Specifies the number of currently active calls for the site.
% Bandwidth Used	Specifies the cumulative bandwidth used by the currently active calls.
Bandwidth	
Avg Bit Rate	Specifies the average bit rate for the currently active calls that is, the total bit rate for all currently active calls divided by the number of active calls.
% Packet Loss	Specifies the average percentage of packet loss for the currently active calls that is, the total percentage of packet loss for all currently active calls divided by the number of active calls.
Avg Jitter	Specifies the average jitter for the currently active calls that is, the total jitter for all currently active calls divided by the number of active calls.
Avg Delay	Specifies the average delay for the currently active calls that is, the total delay for all currently active calls divided by the number of active calls.

2 To view the **Site Statistics** graphically and over a selected period of time:

- a** Click **View Chart**.
- b** In the **Site Name** list, select the site(s) to chart.
- c** In the **Y-Axis** list, select the statistic(s) to chart.
- d** In the **Data Limit** field, enter the time frame in minutes for which to chart the data. The default is 60 minutes.

The charts are dynamically updated for your selections.

Site Link Statistics Report

Use the **Site Link Statistics** report to check call rate and call quality statistics for all site links. You can view the data in a grid or graphically.

To view Site Link Statistics

1 Go to **Reports > Site Link Statistics**.

The **SiteLink Statistics** appear with the statistics displayed in a grid. The grid shows a snapshot of the current statistics. The data is updated automatically every 15 seconds

Column	Description
Site Link Name	Specifies the two linked sites for which the statistics apply.
Num of Calls	Specifies the number of currently active calls for the site link.
% Bandwidth Used	Specifies the percentage of bandwidth used by the currently active calls, that is, the bandwidth used by the currently active calls divided by the total available bandwidth for the link expressed as a percentage.
Bandwidth	Specifies the total bandwidth of the link.
Avg Bit Rate	Specifies the average bit rate for the currently active calls, that is, the total bit rate for all currently active calls divided by the number of active calls.
% Packet Loss	Specifies the average percentage of packet loss for the currently active calls that is, the total percentage of packet loss for all currently active calls divided by the number of active calls.
Avg Jitter	Specifies the average jitter for the currently active calls that is, the total jitter for all currently active calls divided by the number of active calls.
Avg Delay	Specifies the average delay for the currently active calls that is, the total delay for all currently active calls divided by the number of active calls.

2 To view the **Site Link Statistics** graphically:

- a** Click **View Chart**.
- b** In the **Site Name** list, select the site(s) to chart.
- c** In the **Y-Axis** list, select the statistic(s) to chart.

- d** In the **Data Limit** field, enter the time frame in minutes for which to chart the data. The default is 60 minutes.

The charts are dynamically updated for your selections. The site-links are displayed in the same order as the site-link grid.

H.323 Call Detail Records Report

The H.323 Call Detail Record (CDR) report includes CDRs for Polycom and non-Polycom endpoints. Use data from the H.323 Call Detail Record (CDR) report to troubleshoot problems, provide information about network traffic, and ensure accurate billing for video calls.

Notes

- Endpoints that access the CMA system through a Polycom VBP device do not have CDRs.
- Only calls that go through the gatekeeper are included in this report.
- A Call Detail Record is recorded for each IP call into a conference.
- CDR reports may not include data for calls made in the last 24 hours, depending upon when the data in the *localcdr.csv* file was last updated.

To work with the H.323 Call Detail Records report data, extract the report from the *Logger.dbo.calls* database. See your Microsoft SQL Server documentation for information about extracting data.

To view the H.323 Call Detail Records report

- 1 Go to **Reports > H.323 Call Detail Records**.

The **H.323 Call Detail Records** report appears. It lists the CDRs for the 5,000 most recent IP calls made to or from system-managed endpoints. It includes the following information.

Column	Description
Call ID	Specifies the ID automatically generated for the call.
Conf ID	Specifies the GUID (global unique identifier) for the conference to which the call was made.
Date/Time	Specifies the date and time the call started, provided in local time for the server.
Source	Specifies the name, IP, or alias of the endpoint that originated the call.
Source Address	Specifies the IP address of the endpoint that originated the call.

Column	Description
Destination	Specifies the name, IP address, or alias of the endpoint that received the call. For point-to-point calls this is another endpoint. For multipoint calls using an MCU, this is the MCU.
Destination Address	Specifies the IP address of the endpoint that received the call.
Call Type	Specifies the type of call: scheduled or unscheduled.
Bandwidth (Kbps)	Specifies the bit rate that was used for the call.
Duration (min)	Specifies how long the call lasted in minutes, up to a maximum of 999.
Q.850 Code	Specifies the standard cause code for call termination.

- 2 Use the **Filter** to customize the report by **Date**, **IP Address**, **Endpoint Type**, **Call Type**, and **Duration**.

Call Detail Record Report Administration

By default, the CMA system stores the conference and endpoint call detail records (CDRs) for 30 days. You can modify the CDR retention period and you can schedule a weekly archive of the CDRs. These procedures are described in the following topics.

Modify the CDR Retention Period

By default, the conference and endpoint CDRs are purged after 30 days.

To change how long CDR information is retained

- 1 Go to **Admin > Report Administration**.
- 2 In the **Report Administration** page, enter the number of **Days to keep Conference and Endpoint CDRs**.
- 3 Click **Save Settings**.

Schedule Weekly Archives of the CDR Report

To schedule weekly archives of CDR information

- 1 Go to **Admin > Report Administration**.
- 2 In the **Report Administration** page, select **Enable Weekly FTP Archiving of CDR Records**.

3 Configure these settings:

Field	Description
First day of weekly archive	Specifies the day on which the system will transfer archives. By default, this is Sunday. As needed, you can select a different day for the transfers.
Use Secure FTP (SSL/TLS)	Specifies whether or not the archives will be transferred over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection. By default, the system does not secure the transfers.
Host name or IP Address of FTP server	Specifies the server to which the archives will be transferred. By default, the system transfers the archives to a location on its local server. You can change this to an external server.
FTP Port	Specifies the port through which the archives will be transferred. By default, this is system port 21.
FTP User Name/ FTP Password/ Confirm FTP Password	Specifies a user name and password combination for accessing the FTP server. This must be a valid user account on the FTP server.
FTP Directory	Specifies the directory on the server to which the archives will be transferred.

4 To verify that the FTP settings are functional, click **Test Archive Settings**.**5** When the settings are correct, click **Save Settings**.

Endpoint Usage Report

The **Endpoint Usage Report** is based on the CDRs extracted from selected endpoints and includes entries for ISDN and IP calls. (Currently, the CMA system reports CDRs for the Polycom dynamically managed, Polycom non-dynamically managed, HDX Series, RealPresence Group Series, V and VSX Series, VVX, and CMA Desktop endpoints as well as supported TANDBERG and LifeSize endpoint models.)

Use data from the **Endpoint Usage Report** to troubleshoot problems, provide information about network traffic, and ensure accurate billing for Polycom video calls.

To view the Endpoint Usage Report

- 1 Go to **Reports > Endpoint Usage Report**.

The **Endpoint Usage Report** page appears displaying the following information for the endpoints for which CDRs are available.

Field	Description
Serial Number	The registered serial number of the endpoint.
Endpoint Name	The registered name of the endpoint.
Site	The location at which the endpoint resides.
Owner/Room	The person or room to whom the endpoint is registered.

The CDRs are displayed in alphabetical order for the default **Start Date** and **End Date**. By default, the CDRs for the last week are reported.

- 2 To restrict the report to a different time period, change the **Start Date** and **End Date**. The report is dynamically updated.
- 3 Use the **Filter** to customize the report by endpoint **Type**, **Name**, **IP Address**, **ISDN Video Number**, **Alias**, **Site**, or **VIP** status.
- 4 To generate the Endpoint Usage report, select one or more endpoints to include in the report and click **Generate Report**. Use the CTRL key, to select multiple endpoints.

The **Generate Report** page displays the **Summary** usage report for the selected endpoints. It includes the following information for the calls.

Field	Description
Number of calls	Specifies the number of calls the selected endpoints joined for the selected date range. Click Details to get more information about these calls.
Total call time	Specifies the total amount of time the selected endpoints spent in conference during the selected date range.
Average time per call	Specifies the average amount of time the selected endpoints spent in conference during the selected date range, that is, the total call time divided by the number of calls.
Average rate per call	Specifies the average bit rate for the selected calls.

- 5 To select a different group of endpoints, click **Change Selection**, select the endpoints, and click **Generate Report** again.
- 6 Click **Call Times** to see a chart that identifies the number of calls versus the start time for the calls.

- 7 Click **Inbound** to see a chart that identifies the endpoints from which the inbound calls to the selected endpoints originated.
- 8 Click **Outbound** to see a chart that identifies the endpoints to which the selected endpoints called.
- 9 Click **Summary CDR Report** to see a grid that displays information for each of the selected endpoints that participated in calls.

Field	Description
Serial Number	The registered serial number of the endpoint.
Endpoint Name	Identifies the endpoint by name.
Total Time in Call	Specifies the total amount of time the endpoint spent in conference during the selected time period.
Average Time in Call	Specifies the average amount of time the endpoint spent per call during the selected time period, that is, the Total Time in Call divided by the Total Calls .
Average Speed All Calls	Specifies the average bit rate for all of the calls in which the endpoint participated during the selected time period, that is, total bit rate divided by the Total Calls .
Calls Out	Specifies the number of calls in which the endpoint participated during the selected time period that originated from the endpoint.
Calls In	Specifies the number of calls in which the endpoint participated during the selected time period that did not originate from the endpoint.
Total Calls	Specifies the total number of calls in which the endpoint participated for the selected time period.

If any of the selected endpoints did not participate in calls during the selected time period, it is not included in the **Summary CDR Report**.

- 10 To export the information in the **Summary CDR Report**, click **Export as Excel File** and either **Open** or **Save** the file as needed. Note that only the first 1000 lines of the report are exported to the Excel file.
- 11 Click **Detail CDR Report** to see information for each of the endpoints that participated in calls.

The **Generate Report** page displays **System Information** and CDR information for the first endpoint in the list. For the selected endpoint, the **System Information** section includes the following data.

Field	Description
System Information	Specifies the name of the selected endpoint.
Model	Specifies the model number of the selected endpoint.
IP Address	Specifies the IP address of the selected endpoint.
ISDN or V.35 Number	Specifies the ISDN number or V.35 number.
Serial Number	Specifies the serial number of the selected endpoint.

For each call from the selected endpoint, the CDR information includes the following data.

Field	Description
Start Date Time	Specifies the start date and time for the conference.
End Date Time	Specifies the end date for the report. This also defaults to the current date.
Call Duration	Specifies how long the call lasted in hours, minutes, and seconds.
Account Number	If Require Account Number to Dial is enabled on the system, the value entered by the user is displayed in this field.
Remote System Name	Specifies the endpoint to which the endpoint was connected for the call.
Call Number 1 Call Number 2	Specifies the IP or ISDN numbers for the endpoints to which the endpoint was connected for the call.
Transport Type	The type of call — Either H.320 (ISDN), H.323 (IP), or SIP.
Call Rate	The bandwidth negotiated with the far site.
System Manufacturer	The name of the system manufacturer, model, and software version, if they can be determined.
Call Direction	In — For calls received. Out — For calls placed from the system.
Conference ID	A number given to each conference. A conference can include more than one far site, so there may be more than one row with the same conference ID.
Call ID	Identifies individual calls within the same conference.

Field	Description
H.320 Channels	The total number of ISDN B channels used in the call. For example, a 384K call would use six B channels.
Endpoint Alias	The alias of the far site.
Endpoint Additional Alias	An additional alias of the far site.
Endpoint Type	Terminal, gateway, or MCU.
Endpoint Transport Address	The actual address of the far site (not necessarily the address dialed).
Audio Protocol Tx	The audio protocol transmitted to the far site, such as G.728 or G.722.1.
Audio Protocol Rx	The audio protocol received from the far site, such as G.728 or G.722.
Video Protocol Tx	The video protocol transmitted to the far site, such as H.263 or H.264.
Video Protocol Rx	The video protocol received from the far site, such as H.261 or H.263.
Video Format Tx	The video format transmitted to the far site, such as CIF or SIF.
Video Format Rx	The video format received from the far site, such as CIF or SIF.
Disconnect Info	The description of the Q.850 (ISDN) cause code showing how the call ended.
Q850 Cause Code	The Q.850 cause code showing how the call ended.
Total H.320 Errors	The number of errors during an H.320 call.
Avg % Packet Loss Tx	The combined average of the percentage of both audio and video packets transmitted that were lost during the 5 seconds preceding the moment at which a sample was taken. This value does not report a cumulative average for the entire H.323 call. However, it does report an average of the sampled values.
Avg % Packet Loss Rx	The combined average of the percentage of both audio and video packets received that were lost during the 5 seconds preceding the moment at which a sample was taken. This value does not report a cumulative average for the entire H.323 call. However, it does report an average of the sampled values.

Field	Description
Avg Packet Loss Tx	The number of packets transmitted that were lost during an H.323 call.
Avg Packet Loss Rx	The number of packets from the far site that were lost during an H.323 call.
Avg Latency Tx	The average latency of packets transmitted during an H.323 call based on round-trip delay, calculated from sample tests done once per minute.
Avg Latency Rx	The average latency of packets received during an H.323 call based on round-trip delay, calculated from sample tests done once per minute.
Max Latency Tx	The maximum latency for packets transmitted during an H.323 call based on round-trip delay, calculated from sample tests done once per minute.
Max Latency Rx	The maximum latency for packets received during an H.323 call based on round-trip delay, calculated from sample tests done once per minute.
Avg Jitter Tx	The average jitter of packets transmitted during an H.323 call, calculated from sample tests done once per minute.
Avg Jitter Rx	The average jitter of packets received during an H.323 call, calculated from sample tests done once per minute.
Max Jitter Tx	The maximum jitter of packets transmitted during an H.323 call, calculated from sample tests done once per minute.
Max Jitter Rx	The maximum jitter of packets received during an H.323 call, calculated from sample tests done once per minute.

- 12** To export the information, click **Download Report** and either **Open** or **Save** the CDR report in Microsoft Excel format for the selected endpoint or in CSV format **For All Selected Endpoints**. Note that only the first 1000 lines of the report are exported to the Excel file.
- 13** Click **Change Selection** to return to the **Endpoint Usage Report** page to select a different endpoint.

Conference Type Report

Use the **Conference Type Report** option to review monthly summary information about past CMA system conferences.

To create a Conference Type Report

- 1 Go to **Reports > Conference Type Report**.

An empty **Conference Type Report** grid appears.

- 2 As needed, change the **From:** and **To:** dates to select the date range for the report, and click **View**.

The **Conference Type Report** for the selected date range appears. It includes the following information.

Column	Description
Date	Information is displayed on a month-by-month basis and an average for the selected months.
Scheduled Confs	The number of conferences scheduled via one of the CMA system scheduling interfaces (that is, the CMA system application, the Polycom Scheduling Plugin for Microsoft Outlook, or the Polycom Scheduling Plugin for IBM Lotus Notes).
Ad hoc Confs	The number of conferences that used one or more endpoints for which the CMA system was the gatekeeper, but that weren't scheduled via one of the CMA system scheduling interfaces.
MP Confs	The number of multipoint conferences scheduled using one of the CMA system scheduling interfaces.
P2P Confs	The number of point-to-point conferences scheduled using one of the CMA system scheduling interfaces.
Gateway Confs	The number of scheduled conferences that used a gateway to reach one or more endpoints.
Embedded MP Confs	The number of scheduled multipoint conferences that used the MCU embedded in a V-Series, VSX-Series, or Polycom HDX-Series endpoint rather than an external MCU such as an MGC or RMX MCU.
Two Person Conferences on MCU	The number of scheduled point-to-point conferences that used an external MCU such as an MGC or RMX MCU even though point-to-point conferences do not usually require MCU resources.
Short Confs	The number of scheduled conferences that were scheduled to last 30 minutes or more, but which actually lasted less than 30 minutes.

Column	Description
Scheduled Minutes	The sum of the scheduled minutes for all CMA system scheduled conferences.
Executed Minutes	The sum of the actual minutes for all CMA system scheduled conferences.
Total Parts	The sum of the participants that joined CMA system scheduled conferences.
Avg Parts in MP Confs	The average number of participants that joined scheduled CMA system multipoint conferences.

- 3** To create one of the conference type report charts, click the appropriate chart name below the grid. Chart choices include:

Column	Description
Scheduled vs. Ad hoc	A chart that compares the number of scheduled conferences to the number of ad hoc conferences for each month
Scheduled Types	A chart that compares the number of point-to-point, multipoint, gateway, and embedded multipoint conferences for each month
Scheduled vs. Executed Mins	A chart that compares the number of scheduled minutes to the number of executed minutes for each month
Avg Parts in MP Confs	A chart that displays the average number of participants in multipoint conferences for each month
Point-to-Point Confs on MCUs	A chart that displays the number of point-to-point conferences hosted on an external MCU for each month

The selected chart dynamically appears below the grid.

- 4** To export the report:
- a** Click **Export**.
 - b** In the **File Download** dialog box, click **Save**.
 - c** In the **Save As** dialog box, browse to the location to which to save the report and click **Save**.

Gatekeeper Message Log

Use the **Gatekeeper Message Log** page to:

- View messages that endpoints send to the gatekeeper
- Define which messages are logged
- Pause and restart message logging
- Clear the log
- Export the log to another file

Logging starts when you define the **Log Settings**. Logging stops only when you clear all of the **Log Settings**. Logging can include these types of messages:

- **Warnings/Errors.** Messages displayed for all warnings or errors that occur on registered Polycom endpoints
- **Rogues.** Messages displayed for all calls from unregistered endpoints
- **Events.** Messages display about these events:
 - Registration
 - Call detail
 - Neighboring gatekeeper

While you can pause logging, the CMA system always logs errors and warnings.

You can also:

- Clear events from the log, which removes data from the database
- Export the log to a comma-separated value (CSV) file. You can export only the data that displays on-screen, and exporting the log may take a long time depending on the number of entries in the log.

View and Export the Gatekeeper Message Log

To see more details about a log message

- 1 Go to **Reports > Gatekeeper Message Log**.
- 2 Enter a **Filter String** to customize the list.
- 3 Select the message of interest.

The **Gatekeeper Message Log** report appears. It has these fields:

Column	Description
Type	<p>These types of messages display:</p> <ul style="list-style-type: none"> Information, which indicates normal communications between the CMA system and the endpoint. Warning, which indicates an unscheduled call and the inability to assign E.164 and ISDN numbers to an endpoint. Error, which indicates the registration of an endpoint or a call failed, or a lack of resources for this gateway or MCU exists.
Date/Time	Date and time of the event.
Category	Specifies whether an event is a registration, call, or neighboring gatekeeper request.
Description	Displays the message sent to or received from the endpoint, identified by the IP address.

- 4 To export a message:
 - a Select the message of interest and click **Export Log**.
 - b In the **Export Log** dialog box, click **Yes**.
A *GKexport file* appears in your default text editor.
 - c Save the file.

Define Log Settings

To define which messages should be logged

- 1 Go to **Reports > Gatekeeper Message Log**.
- 2 When the **Gatekeeper Message Log** page appears, click **Log Settings**.
- 3 In the **Gatekeeper Log Settings** dialog box, select the events to log.

Field	Description
Registration	
RRQ	Registration requests
GRQ	Gatekeeper requests
IRR/IRQ	Information response or information sent
LWRRQ	Light-weight registration request

Field	Description
URQ	Unregistration request
Non Standard Message	
Neighbors	
LRQ	Location request
Call Details	
ARQ	Admission request
DRQ	Disengage request
BRQ	Bandwidth request
Setup	

4 Click **OK**

The CMA system begins logging the types of messages you selected.

Clear Events from the Log

To clear all events from the log

- 1** Go to **Reports > Gatekeeper Message Log**.
- 2** When the **Gatekeeper Message Log** page appears, click **Clear Log**.
- 3** Click **Yes** to confirm the action.

The **Gatekeeper Message Log** is cleared.

Pause and Restart Logging

To pause logging

- 1** Go to **Reports > Gatekeeper Message Log**.
- 2** When the **Gatekeeper Message Log** page appears, click **Pause Log**.
- 3** In the **Stop Logging** dialog box, click **Yes**.

The **Start Log** button is available and the system stops logging messages to the **Gatekeeper Message Log**.

- 4** Click **Start Log** to restart logging.

Many of the CMA system components can write a **System Log File** when they experience an error or issue. Whether or not they do write a system log file depends upon the system log level.

The following table lists some of the logs the CMA system saves.

Log Name	Description
Log Files Related to Basic System Functionality	
SE200MasterService.txt	Log file that shows when individual services are started and stopped, and displays a memory usage summary for some of those services (mqm, sitetopo, plcmgk, gab) every 30 minutes.
ESINSTALL-<timestamp>.txt	Log file that shows the output of the CMA system install script. Shows what steps were done when installing the CMA system software.
ESUPGRADE-<timestamp>.txt	Log file that shows the output of the CMA system upgrade script (not applicable unless an upgrade was performed).
Log File Related to Dial Plan Functionality	
DialRule_Log.txt	General log file used by the dial rule process. This process generates dial out strings to endpoints, controls the dialing rules set up in the user interface.
SiteTopo_Log.txt	When in debug mode, this log file contains messages about site topology entry and usage.
Log File Related to External Database Functionality	
ServiceMonitor_Log.txt	Log file for the redundancy service that shows when a redundant CMA system goes into active or standby mode.
Log Files Related to Scheduling Functionality	
AdapterLog_SCH.txt	.NET remoting log file that shows low-level communication errors between internal system components--in this case, the scheduling component.
Log Files Related to Global Address Book Functionality	
AdapterLog_GAB.txt	.NET remoting log file that shows low-level communication errors from the GAB communications with the integration layer.

Log Name	Description
ComponentLog_GAB.txt	.NET remoting log file that shows low-level communication errors from the GAB communications with endpoints.
EXXX_LOGx.txt	Log files for web services, device manager, and conference monitoring. This file includes information about successful and failed system logins and all logouts, as well as system errors, major system events, and general system information.
Log Files Related to Device Management Functionality	
AdapterLog_GMS.txt	.NET remoting log file that shows low-level communication errors between internal system components--in this case, the management component.
<DeviceType>Device.txt	Log file that captures device specific message.
<DeviceType>DeviceCollection.txt	Log file that captures device specific message.
<DeviceType>PasswdErrs.log	Log file that captures device specific messages related to potential password mismatches.
DeviceManager.txt	Log file for the device management process.
DeviceManagerService.txt	Log file for the device management process.
softwareUpdate	Log file that shows when an endpoint is updated with a new software package via a scheduled software update.
Log Files Related to Gatekeeper Functionality	
AdapterLog_PN.txt	.NET remoting log file that shows low-level communication errors between internal system components--in this case, the gatekeeper component.
PLCMGK.log	General gatekeeper log file.
MQM_Log.txt	General media quality monitor log file that will show any errors when writing CDRs or media quality data to the database.

Log Name	Description
Log Files Related to Call Management Functionality	
Messages.txt	Conference launching log used exclusively by CodecMngr process. This log contains information about the conference start up process, that is, information that the system sends to endpoints at the start of a conference.
CS_<conf_name>.html CS_<conf_name>.txt	Conference scheduling log used by the conference scheduling process. This log contains debug information on how a conference is created. A log file is created for each scheduled conference, with the log file name format: CS-<conf_name>.txt, where <conf_name> is the name of the scheduled conference. This is always on, and there is no logging level.
Log Files Related to Web Services Functionality	
apache_access.log.<xxxx>	Apache web server access log that shows when and what URL was requested.
apache_error.log	Log file that captures error messages from the Apache web server.
mod_jk.log	Log file that shows which web requests were forwarded from Apache web server to the Tomcat servlet engine.
Log Files Related to Presence Functionality	
Jserver.log.<n>	Log file that shows errors related to the internal LDAP, SNMP, DM, Openfire, Site Topology and dynamically-managed endpoint login and provisioning functionality. This circular log has a six month limit. The timestamp is the local server time.
boot.log	JBoss startup log. JBoss is the container service for the Jserver service.

View and Export System Log Files

Many of the CMA system components can write a **System Log File** when they experience an error or issue.

Whether or not they do write a system log file depends upon the system log level. You can change the system log level. See [“Change the System Log Level”](#) on page 300.

To view System Log Files

- 1 Go to **Reports > System Logs**.

The **System Log Files** list appears listing the logs for the given time period.

- 2 To view a log file:

- a Select the log file of interest.
- b Click **Open**.

- 3 To export a **.zip** of all log files:

- a Click **Download All**.
- b To open the **.zip** file, in the **File Download** dialog box, click **Open with**, and browse to the program you use to open **.zip** files.
- c To save the **.zip** file to your local computer, in the **File Download** dialog box, click **Save**.

Change the System Log Level

To edit the current system log level

- 1 Go to **Reports > System Logs**.

The **System Log Files** list appears listing the logs for the given time period. The **Current Log Level** indicates which log files are being saved.

- 2 Select the report you want.

- 3 Click **Change Settings**.

- 4 From the **Current Log Level** menu, select a new value. Choices include:

- Debug
- Info
- Warn
- Error
- Fatal
- Off

- 5 In a redundant configuration, repeat steps 1 and 4 on the redundant server.

Download Windows Event Log Files

You can download a .zip file that includes the Windows Event Log Files for the CMA system. The Windows Event Log Files include the operating system level application, security, and system logs. These logs store events logged by Windows system components.

To download the Windows Event Logs

- 1 Go to **Reports > System Log Files**.
- 2 Click **Download All Event Logs**.
- 3 In the **File Download** dialog box, click **Save** to save the log file to your local system.

View and Download Audit Log Files

You can view and download audit log files.

To view and download audit log files

- 1 Go to **Reports > Audit Log Files**.

The **Audit Log Files** page appears listing the logs being stored on the system. The following table identifies the CMA system audit log files.

Log Name	Description
apache_access.log.<timestamp>	Log file that shows every web request that was made from client systems. The system may have more than one such log.
apache_error.log	Log file that captures all of the failed web requests as well as any internal Apache error messages.
cma_audit_ComponentLog_ApacheCert1.log	Log file that captures security-related authentication issues.
cma_audit_EXXX_LOG1.log	Log file that captures significant .NET application events.

Log Name	Description
cma_audit_jserver.log	Log file that captures significant Java Server application events.
cma_audit_os_patches_hotfixes1.log	Log file that is created when the system first starts up. It displays the operating system updates and hotfixes applied to the CMA system.
ntp.log	Log file that captures time server related events.
opens-access-log.txt	Log file that captures activity queries sent to OpenDS.
opens-audit-log.txt	Log file that captures OpenDS configuration events.
opens-replication-log.txt	Log file that captures redundancy and DMA system integration events. Not available because redundancy and DMA integration are not supported.

- 2 Select the audit log of interest and click **Open**.
- 3 In the **File Download** dialog box, click **Open** to view the file or click **Save** to save the log file to your local system.

Backup and Delete Audit Log Files

You can backup and delete audit log files.

To backup and delete audit log files

- 1 Go to **Reports > Audit Log Files**.
The **Audit Log Files** page appears listing the logs being stored on the system.
- 2 Click **Backup and Delete**.
- 3 In the **Backup and Delete** dialog box, select the checkboxes of the log files to backup.
- 4 Click **Backup** to begin backing up the log files into a zip folder.
- 5 Click **Save**.
- 6 In the **Backup and Delete** dialog, click on **Download Verification Utility**, if it is not installed already.

- 7 To enter the verification code, leave the dialog open, until you get the verification code from the File Verification Utility.
- 8 Run the File Verification Utility.
- 9 In the File Verification Utility dialog box, browse to the location of the backed-up file and select it, the utility will run when the file is selected.
After the utility runs, a verification code will be visible in the Verification Value field.
- 10 In the File Verification Utility dialog, click **Copy**.
- 11 In the Backup and Delete dialog, click in the **Verification Code** field and press CTRL-V to paste in the Verification code into the field.
- 12 Click on **Verify and Delete**. The backed-up file will be checksum verified and the backed-up log files will be deleted.



Note

It is important for the user to log into the CMA system with the proper roles to be able to view and access the **Backup and Delete** option, otherwise only the **Open** option will be visible.

The alerting threshold may be modified through the **Change Settings** option.

CMA System Report

The **CMA System Report** is not available from the Reports menu, but it can be a useful report. It produces a *SystemInfo.txt* file that describes the system configuration.

To view CMA System Report

- 1 Go to **Admin > Troubleshooting Utilities**.
- 2 In the **CMA System Report** section of the **Troubleshooting Utilities** page, click **Download Report** in the **CMA System Report** section.
- 3 When the **File Download** dialog box appears, either **Open** or **Save** the *SystemInfo.txt* file:

The report includes this information.

CMA VERSION

```
Software version : 6.00.00.ER012
Hardware version : REVISION_B
LDAP Integration : true
```

SECURITY SETTINGS

System under Secure Mode: false

NETWORK CONFIGURATION

System name : POLYCOM-De11150
System IPv4 Address : 10.47.10.150
System IPv6 Address : N/A
System IPv6 Link local: N/A
System subnet mask : 255.255.255.0
System default gateway: 10.47.10.10
System DNS domain : pe.com
System DNS server 1: 10.47.10.189
System DNS server 2: N/A

LICENSE INFO

Total number of licenses : 100
Number of licenses in used: 10

CONFERENCE SETTINGS

Conference Time Warning : true
Include Conference Owner in new Conference: false
Allow Overbooking of dial-In participants : false
Conference PIN Length : 15

SESSION MANAGEMENT SETTINGS

Remote Desktop Connection is allowed : true
CMA User Interface timeout (in sec) : 60
Max number of sessions per user : 5
Max number of sessions per user enabled : false
Max number of sessions per system : 50
Max number of sessions per system enabled: false

LOCAL USER ACCOUNT CONFIGURATION

Failed login threshold : 3
Failed login windows (hours) : 1
Lockout duration (minutes) : Indefinite
Account Inactivity threshold (days): 30

LOCAL PASSWORD REQUIREMENTS

Maximum password age (days) : 180
Password warning interval (days): 7
Number of lowercase letters : 1
Number of uppercase letters : 1
Minimum length (characters) : 8
Minimum password age (days) : 1
Number of numbers : 1
Reject previous passwords : 8
Number of special characters : 1
Minimum number of changed characters : 1
Maximum consecutive repeated characters: 1

CERTIFICATE INFO

Certificate Common Name : CMA Self-Signed Certificate
Certificate CRL Version : 0
Certificate CRL Expired : false
Certificate Alias :
1.2.840.113549.1.9.1=#1613737570706f727440706f6c79636f6d2e636f6d,c
n=cma self-signed
certificate,ou=vsg,o=polycom,l=pleasanton,st=california,c=us
Certificate Issuer : CMA Self-Signed Certificate

PRIMARY GATEKEEPER INFORMATION

GateKeeper Id : PN:PLCM
GateKeeper description : ReadManager
GateKeeper Registration mode : ALL_ENDPOINTS
GateKeeper deny rogue calls : false
GateKeeper log rogue calls : true
GateKeeper Statistics enabled: false
GateKeeper Registration timeout (days) : 30
GateKeeper Registration refresh (seconds): 300

REDUNDANCY INFORMATION

Server 1 IP address: 10.47.10.150
Server 1 is PRIMARY: true
Server 1 is ON : true
Server 2 IP address: N/A
Server 2 is PRIMARY: false
Server 2 is ON : false
Virtual IP address : N/A

DATABASE CONFIGURATION

Use external DB : false

System Administration Overview

This chapter describes the Polycom® Converged Management Application™ (CMA®) system **Dashboard**, menu, and actions. It includes these topics:

- [Polycom CMA System Dashboard](#)
- [Dashboard Buttons](#)
- [Dashboard Panes](#)
- [System Administration Menu](#)

Polycom CMA System Dashboard

When you log into the CMA system with **Administrator** role and permissions, the system first displays the system **Dashboard**. Use the system **Dashboard** to view information about system health and activity levels.





Note

We recommend that you use a minimum monitor display of 1280 x 1024 pixels to view the system **Dashboard**.

The system **Dashboard** displays data in an array of charts, forms, data grids, and other graphical displays. It is supremely customizable. You can modify your system **Dashboard** layout by moving (select the pane title, hold, drag and drop), minimizing, maximizing, closing, and restoring panes. Also note that your changes to the system **Dashboard** are persistent not just for a session but between logouts and logins.

Dashboard Buttons

In general, the system **Dashboard** displays information only. However, the following buttons are available from the **Dashboard** view.

Button	Use this button to....
Add Panes	Add additional display panes to the system Dashboard . See “Dashboard Panes” on page 308.
Refresh	Update the page with current information. To change the frequency of automatic screen refreshes from the default of 5 seconds, click the down arrow and select another option: 15, 30, 45, or 60 seconds. The Refresh button flashes when the system refreshes the Dashboard or when you click Refresh .
Restart 	Shuts down and restarts the CMA system. See “Restart or Shut Down a Polycom CMA System” on page 6.
Shutdown 	Shuts down the CMA system. See “Restart or Shut Down a Polycom CMA System” on page 6.

Dashboard Panes

By default the system **Dashboard** displays the following informational panes:

- [Users Logged In](#)
- [CMA Configuration](#)
- [CMA Info](#)
- [Services](#)
- [Gatekeepers](#)
- [CMA Licenses](#)

But you can add or remove panes to customize the system **Dashboard**. Additional panes that you can add include:

- [Pre-call Status](#)
- [Today's Adhoc Conferences](#)
- [Today's Scheduled Conferences](#)
- [Endpoints](#) (multiple, configurable panes)
- [Systems](#)
- [Conference Status](#)
- [Failed Enterprise Directory Login Attempts](#)
- [Redundancy Status](#)
- [MCU Status](#) (multiple, configurable panes)

These panes are described in more detail in the following topics.

Users Logged In

The **Users Logged In** pane displays the type and number of users that are currently logged into the system. A sparkline presents the number of logins over time (30 minutes total; updated every 5 minutes so there are 6 data points on the sparkline) for each user type.

The system identifies three user types by their permissions: **Administrators**, **Operators**, and **Schedulers**.

Note that these three user types are not necessarily the same as user roles. For example, users assigned the default **Administrator** and default **Device Administrator** roles appear in this pane as **Administrators**. And users assigned the default **View Only Scheduler**, default **Scheduler**, and default **Advanced Scheduler** roles appear in this pane as **Schedulers**.

For more information, see [“Roles and Permissions”](#) on page 252.

CMA Configuration

The **CMA Configuration** pane displays information about the configuration of the CMA system, including:

Field	Description
Software Version	Displays the current version of CMA system software running on the system.
Hardware Version	The hardware of the CMA system.
CMAD Shipped Version	Displays the version of CMA Desktop for PC that shipped with the version of CMA system software running on the system. Users can download this version of the Polycom CMA Desktop software from the Downloads page.
CMAD Mac Shipped Version	Displays the version of CMA Desktop for Macintosh that shipped with the version of CMA system software running on the system. Users can download this version of the Polycom CMA Desktop software from the Downloads page.
Enterprise Directory	Displays the enterprise directory configuration. Possible values include: <ul style="list-style-type: none"> Auto—If the system is configured to auto-discover the enterprise directory server. DNS name or IP address of the enterprise directory server—If an enterprise directory server is specified on the system configuration page. None—If the system is not integrated with an enterprise directory server.
Database	Displays the database source (Internal or External) and the DNS name or IP address of the database server.

Field	Description
Time Source	Displays the time server source (Internal or External) and the IP address of the time server.
Redundancy	Displays whether or not the system is configured for redundancy. The Redundancy field may also show two configuration errors: Need Virtual IP or Secondary Is Down .
Remote Alerts	Displays whether or not the system is configured to send remote alert notifications.
Enterprise Directory DC	If the system is integrated with a domain controller for single sign on authentication, displays the domain name for that domain controller. If the system is not integrated with a single sign on domain controller, this field displays Disabled .
Remote Desktop	Displays whether or not Remote Desktop Connection is enabled.

CMA Info



The **CMA Info** pane displays general information about the CMA system, including:

Field	Description
CPU Utilization	Displays two views of the CMA system control processor unit (CPU) usage: <ul style="list-style-type: none"> A sparkline that presents the CPU usage over time (10 minutes total; updated every 1 minute so there are 10 data points on the sparkline) A percentage indicator that shows the current usage
Paging File	Displays two views of the CMA system paging file usage: <ul style="list-style-type: none"> A sparkline that presents the paging file usage over time (10 minutes total; updated every 1 minute so there are 10 data points on the sparkline) A percentage indicator that shows the current usage
Last Hard Start/Reboot	Displays the date and time of the last complete system start.
Provisioning in Progress	Displays the number of scheduled endpoint provisioning processes that are currently underway.
Software Updates in Progress	Displays the number of scheduled endpoint software update processes that are currently underway.
Hardware Alarms	The number of hardware components in the CMA system reporting a warning state.
Threshold Alarms	The number of hardware components in the CMA system reporting an error state

Field	Description
Total Memory	The total amount of RAM on the CMA system.
Free Memory	The amount of free RAM space on the CMA system.
Partition [C:] Memory	The amount of used and unused capacity on the CMA system partition C.
Partition [D:] Memory	The amount of used and unused capacity on the CMA system partition D.
Partition [E:] Memory	The amount of used and unused capacity on the CMA system partition E.
Temperature	Temperature status information provided by the Polycom-branded Dell server agent through its MIB
Power Supply Status	Power supply status information provided by the Polycom-branded Dell server agent through its MIB
Battery Status	Battery status information provided by the Polycom-branded Dell server agent through its MIB
Cooling Fan	Fan status information provided by the Polycom-branded Dell server agent through its MIB

Services

The **Services** pane displays information about the CMA system services, including:

- How many services are running
- How many services are stopped
- A list of the services and a graphical indicator for each service indicating its state: **Running**  or **Stopped** . If a service is stopped, select the service and a dialog box appears that describes the error, possible reasons for the error, and suggestions to correct the error. Click the start service icon to restart the service.

The following table lists the services, their purpose, and whether or not they are essential to the health of the system.

Service	Manages the system's...	Comment
Apache2	Web processes	Essential
MSSQLSERVER	Database processes	Essential
OpenDS	Site topology database	Required for site topology functionality
Polycom Cascader	Cascaded conferencing processes	Required for cascading conferences

Service	Manages the system's...	Comment
Polycom Conference Scheduling Service	Conference scheduling processes	Essential
Polycom Device Manager	Device management processes	Essential
Polycom DialRuleService	Dial rule management processes	Essential
Polycom Gatekeeper	Gatekeeper processes	Essential
Polycom JServer	Java processes including LDAP, SNMP, device management, Site Topology, and dynamically-managed device logins and provisioning.	Essential
Polycom Master Service	Basic operation processes	Essential
Polycom Serial COM	Serial port management processes	Essential
Polycom Service Monitor	Redundancy monitoring processes	Required for redundancy

When users log into a CMA system, the system first checks to make sure all essential services are running before allowing users to access the system. The following situations may occur.

- If all essential services are running, users are allowed to access the system.
- If one or more essential services is down, and the Apache service has been running for less than seven minutes, users receive an error message saying, "The CMA system is not ready. Please try again in a few minutes."
- If one or more essential services is down, but the Apache service has been running for at least seven minutes, users are allowed to access the system. In this case, specific system functions may be unavailable to users.

Gatekeepers

The **Gatekeepers** pane displays information about the CMA system as a gatekeeper, including:

Field	Description
Gatekeeper Statue	Displays the status of the CMA system gatekeeper. Possible values are Up or Down .

Field	Description
Call Model	Describes how the CMA system routes selected H.225 call signaling messages. Possible values include: Routed or Direct . For more information, see “Routing Mode” on page 398.
Neighbors	Displays the number of neighboring gatekeepers identified for the CMA system.
Alternate Configured	Displays whether or not the CMA system has an alternate gatekeeper identified.
Registered Devices	Displays the number of devices currently registered to the CMA system gatekeeper.
Active Calls	Displays two views of the current CMA system active calls: <ul style="list-style-type: none"> A number field that shows the current number of active calls A graph that presents the percentage of active calls over time
Maximum Allowed	The maximum number of active calls. This value is dependent on the call model (routed or direct) and the total number of licenses <ul style="list-style-type: none"> In routed mode, the maximum number of active calls is 30% of the total number of licenses. In direct mode, the maximum number of active calls is 60% of the total number of licenses.

CMA Licenses

The **CMA Licenses** pane displays information about how the CMA system is licensed, including:

- The **Total Number of Licenses** available on the system
- The **Licenses in Use**, which displays two views of the CMA system active calls:
 - A sparkline that presents the license usage over time (60 minutes total; updated every 5 minutes so there are 12 data points on the sparkline).
 - A percentage indicator that shows the current usage.

Pre-call Status

The **Pre-call Status** pane displays information about the next conference or conferences that are scheduled to launch including:

Field	Description
Time to Conference	Displays the system-defined pre-call status reporting time of 10 minutes. In other words, the Pre-call Status pane always reports on conferences that are scheduled to start in the next 10 minutes.
Scheduled to Launch	Displays the number of conferences scheduled to start in the next 10 minutes.

Field	Description
Ready to Launch	Displays the subset of conferences that are scheduled to start in the next 10 minutes and that have passed the resource tests that the system executes before launching a conference.
Ready to Launch with Device in Call	Displays the subset of conferences that are scheduled to start in the next 10 minutes and that have passed the resource tests but that still have one or more devices in another call.
NOT Ready to Launch	Displays the subset of conferences that are scheduled to start in the next 10 minutes but that have not yet passed the resource tests. Also displays the conferences that are not ready to launch.

Today's Adhoc Conferences

The **Today's Adhoc Conferences** pane displays information about the ad hoc conferences started by video endpoints registered to the CMA system. For the current day (starting at 0:00 and ending at 24:00), it displays:

- The number of ad hoc conferences that were **Completed** for the current day
- The number of ad hoc conferences that are **Active** at the current time
- A bar chart that displays the number of ad hoc conferences (vertical axis) plotted against time of day (horizontal axis)

Today's Scheduled Conferences

The **Today's Scheduled Conferences** pane displays information about the scheduled conferences managed by the CMA system. For the current day (starting at 0:00 and ending at 24:00), it displays:

- The number of scheduled conferences that were **Completed** that day
- The number of scheduled conferences that are **Active** at the current time
- The number of scheduled conferences that are yet to occur (**Future**)
- A bar chart that displays time on the linear axis plotted against the number of scheduled conferences on the horizontal axis

Endpoints

The system allows you to add multiple **Endpoints** panes so you can create your own scheme for grouping and monitoring endpoints. When you add an **Endpoints** pane, you can give the pane a meaningful name and select which endpoints to monitor. You can save the pane, create others as needed. You can also reconfigure an **Endpoints** pane using the configuration tool.

Endpoints panes display the following information:

- The number of endpoints being monitored
- The number of monitored endpoints that are **In a Call**

- The number of monitored endpoints that are **Online**
- The number of monitored endpoints that are **Offline**

In addition, the **Endpoints** pane identifies any monitored endpoints that are experiencing alert conditions. If you click on an endpoint in the list, the system displays the **Endpoint > Monitor View**.

Finally, click **View Endpoint** to see the **Status**, **Name**, **Alias**, **IP Address**, **Owner**, and **Site** for the monitored endpoints. This status information is sent by the endpoints to the CMA system.

Systems

The **Systems** pane displays summary information about the devices registered with the CMA system, including:

Field	Description
Endpoints	The number of endpoints registered with the CMA system.
VVXs	The number of VVX systems registered with the CMA system.
MCUs	The number of MCUs registered with the CMA system.
Gatekeepers	The number of neighbored gatekeepers identified to the CMA system plus the CMA system itself.
Gateways	The number of individual H.323 cards and/or IP blades in Polycom MCUs are assigned the device type of GW/MCU during registration. For more information, see "Network Device Types" on page 221.
Rooms	The number of rooms defined with the CMA system.
VBPs	The number of VBPs defined with the CMA system.
DMAs	The number of DMAs defined with the CMA system.
Touch Controls	The number of Touch Controls defined with registered endpoints.

If any of the devices registered with the CMA system experience a fault, the **Systems** pane also displays an alert icon. Click the alert icon to see the **Endpoint** or **Network Device** view and get more information about the alert.

Conference Status

The **Conference Status** pane displays the list of active conferences, plus 2 of 6 participants online.

Click on conference title to go to conference monitor view for that conference.

Failed Enterprise Directory Login Attempts

The **Failed AD Login Attempts** pane displays:

- The total number of **Failed Logins** for Active Directory users in the last 24 hour period.
- The domain\username for the Active Directory users whose login attempts failed and how many times they failed. Click the domain\username to view the date and time for the failed attempts.

Redundancy Status

The **Redundancy Status** pane displays information about the CMA system redundancy configuration, including:

- Whether or not the system is configured for redundancy. Possible values for Status are **Configured** or **Not Configured**.
- The **Virtual IP Address** for the redundant system
- The IP address of the **Active Server**
- The IP address of the **Backup Server**

MCU Status

The system allows you to add multiple **MCU Status** panes so you can create a pane for all or individual MCUs registered with the CMA system. When you add an **MCU Status** pane, you can give the pane a meaningful name and either select an MCU to monitor or select All MCUs. You can save the pane, create others as needed. You can also reconfigure an **MCU Status** pane using the configuration tool.

The **MCU Status** pane for **All MCUs** displays the following information:

Note

Areas may affect an administrator's ability to **View Details** for an MCU. The administrator and MCU must be assigned to a common area.

Field	Description
Errors	Displays the cumulative number of alarms for all of the registered MCUs.
Warnings	Displays the cumulative number of warnings for all of the registered MCUs.
Active Conferences	Displays the total number of active conferences being hosted by all of the registered MCUs.

The **MCU Status** pane for **All MCUs** also lists all of the registered MCUs and displays the Errors and Warnings for the MCUs.

The **MCU Status** pane for an individual MCU displays the following information:

Field	Description
Errors	Displays the number of alarms on the MCU.
Warnings	Displays the number of conferences that are active on the MCU at the current time.
Active Conferences	Displays the number of active conferences currently being hosted by the MCU.
Number of Audio Ports	Displays the number of dedicated audio ports configured on the MCU.
Audio Ports Utilization	Displays two views of the MCU audio port usage: <ul style="list-style-type: none"> A sparkline that presents the audio port usage over time A percentage indicator that shows the current usage
Number of Video Ports	Displays the number of video ports configured on the MCU.
Video Ports Utilization	Displays two views of the MCU video port usage: <ul style="list-style-type: none"> A sparkline that presents the video port usage over time A percentage indicator that shows the current usage
Expected Port Utilization	A timeline that shows how many ports are scheduled for conferences within the next 45 minutes.

This status information is sent by the MCU to the CMA system.

In addition, the **MCU Status** pane identifies when the monitored MCU is experiencing alert conditions.

System Administration Menu

The system **Admin** menu gives users with administrative permissions access to the day-to-day management tasks they need to monitor, maintain, and troubleshoot the CMA system. Besides the **Dashboard**, it lists these selections:

Selection	Use this selection to...
Conference Templates	Manage (add, edit, and delete) conference templates. See “Conference Templates” on page 321.
Conference Settings	Enable or disable Conference Auto-launch and Conference Time Warning. See “Conference Settings” on page 334.
Provisioning Profiles	Manage (add, edit, and delete) automatic or scheduled provisioning profiles.

Selection	Use this selection to...
Software Updates	Manage (add, edit, and delete) automatic or scheduled software update packages.
Rooms	Manage (add, edit, and delete) rooms in the CMA system directory.
Areas	Manage Areas for a CMA system.
Directories	Manage the directories available to the CMA system including the enterprise directory, address books, or Global Address Book.
Server Settings	Configure the basic CMA system, which includes the network, system time, database, directory, licensing, redundancy, branding, GAB, remote alert, and E-mail set up.
SNMP Settings	Manage SNMP messaging for the CMA system.
Gatekeeper Settings	<p>By default the CMA system is made the default gatekeeper during the First Time Setup process. Use the Gatekeeper Settings option to modify this setting or to add an alternate gatekeeper or neighboring gatekeepers.</p> <p>Gatekeeper Settings affect how devices register and calls are made in your video communications network. These settings allow you to:</p> <ul style="list-style-type: none"> • Identify the gatekeeper with an identifier and description. • Specify registration-related settings, including the default gatekeeper, which endpoints register, the registration refresh period, and the offline timeout. • Set the maximum number of neighboring gatekeeper hop counts. • Specify how to handle calls to and from unregistered endpoints.
Management and Security	Upgrade the CMA system and configure the certificate, security, and endpoint management set up.
Dial Plan and Sites	Edit the default CMA system Dial Plan and Site settings (which includes the definition of sites, site links, dial rules, services, and least-cost routing tables) to support your network topology and video call routing.
Alert Settings	Configure the CMA system to send E-mail alerts for specified system or endpoint events.
Backup System Settings	Download a .zip archive file containing all configuration information necessary to restore the system.
Database Backup Files	View or backup the CMA system internal database backup file.

Selection	Use this selection to...
Uploads	Upload SIP URI data to the CMA system.
Troubleshooting Utilities	Access all of the troubleshooting information and utilities the CMA system has available.
Report Administration	Configure report administration settings including retention periods, etc.

Conference Setup Overview

This chapter describes information about conference templates, options, and settings within the Polycom® Converged Management Application™ (CMA®) system. Two types of configuration settings relate to scheduled conferences:

- [Conference Templates](#) define most of the settings that become the defaults for a conference.
- [Conference Settings](#) are global system-wide settings that apply to all scheduled conferences.

Conference Templates

Conference templates allow you to create various combinations of settings to apply to scheduled conferences.


- For scheduled conferences that end on MGC devices, the conference template explicitly identifies the settings the MGC should use to control the conference.
- For scheduled conferences that end on RMX devices, the conference template explicitly identifies the RMX profile which identifies the settings the RMX should use to control the conference.

Users assigned the **Administrator** role can add or edit **Conference Templates**. They can also identify (by user role) which users have access to which **Conference Templates** and which users have the **Advanced Scheduler** role. Then users select from the different templates available to them to switch between different combinations of conference settings.

If using an existing profile on the RMX system, the CMA system administrator must manually synchronize the settings in the CMA system conference template and its associated RMX profile.

Alternatively, you can configure the RMX profile settings in the CMA system conference template, which is used by all RMX systems in the conference. For more information about the RMX profile settings, see the *Polycom® RMX® 1500/2000/4000 Administrator's Guide*.

Field	Description
General Settings	
Name	Enter a unique and meaningful name for the template, which can be up to 32 characters long.
Description	Enter a meaningful description (ASCII only) of the conference settings template.
Audio-Only Template	Select this option to designate the template as an audio-only template. Selecting this option disables many settings.
Supported MCUs	Specify the supported MCU type. Possible values include: <ul style="list-style-type: none"> • MGC • RMX
Always Use MCU	When selected, an MCU is used for the scheduled conference, regardless of the number of participants. When not selected, an MCU is used only when necessary.
Dial Options	These settings apply only to video conferences. The video dial options are: <ul style="list-style-type: none"> • Dial-In Only (all participants dial into the conference) • Dial-Out Only (all participants are called by the system) • Dial-In + Dial-Out (The person setting up the conference can specify which participants must dial into the conference and which participants are called by the system.)
Template will be available to users with the selected roles...	Select the roles to which users must be assigned for them to see this template when scheduling conferences.
Available Roles	The list of roles defined to the CMA system.
Selected Roles	The list of roles that can use the conference template being defined.
Common Settings	
Meet Me Per Conference	When selected, only one dial-in number is assigned to the conference. When cleared, each dial-in participant is assigned a different dial-in number.

Field	Description
Video Mode	<p>Sets the video layout for the conference. The default is Video Switching Mode.  To change to a Continuous Presence layout or mode, click the switching icon and select a layout option.</p> <p>The video mode determines the initial layout on an endpoint's display during a multipoint conference. This option requires an MCU.</p> <p>This option is not available for RMX devices if you select any of the following:</p> <ul style="list-style-type: none"> • Auto layout option (RMX Video Settings) • Video switching option (RMX General Settings) • Telepresence mode is On (RMX Video Settings) <p>Note</p> <p>Make sure you have defined video endpoint systems and boards so that they are available for selection in continuous presence layouts.</p>
Presentation Mode	<ul style="list-style-type: none"> • Select to enable Presentation Mode. In this mode, the system uses the selected layout to display all participants. When a participant's speech exceeds a predefined time (30 seconds), the system identifies the participant as the lecturer and changes to Lecture Mode. The video mode for the other participant's automatically changes to full screen, displaying the lecturer, while the lecturer's endpoint displays participants in the video mode defined previously. When another participant starts talking, the system changes back to Presentation Mode and the conference returns to its predefined video layout. • Clear this option to disable Presentation Mode. All participants see the conference in the video mode defined elsewhere. <p>This option is not available if you select any of the following:</p> <ul style="list-style-type: none"> • Video switching option (RMX General Settings) • Same layout option (RMX Video Settings) • Telepresence mode is On (RMX Video Settings) <p>Notes</p> <ul style="list-style-type: none"> • RMX 1000 systems do not support Lecture Mode, Presentation Mode, or Lecture View Switching.

Field	Description
Speed (Kbps)	<p>Sets the speed for the conference, which applies to both point-to-point and multipoint calls. Possible values for Polycom MGC systems are between 96 to 1920 Kbps and Bridged Audio. The default is 384 Kbps.</p> <p>Note</p> <p>If you use an RMX profile for conferences that land on an RMX system, the speed designated here is used to reserve bandwidth and must match the line rate defined in the RMX profile that is identified in the Profile Name field.</p>
Lecturer View Switching	<p>Select this option to enable automatic switching of participants on the Lecturer's screen when Lecture Mode is set to Presentation Mode and the number of participants exceeds the number of windows identified by the video mode defined elsewhere.</p> <p>This option is not available if you select any of the following:</p> <ul style="list-style-type: none"> • Same layout option (RMX Video Settings) • Telepresence mode is On (RMX Video Settings) <p>Note</p> <p>RMX 1000 systems do not support Lecture Mode, Presentation Mode, or Lecture View Switching.</p>
MGC Settings	
Entry Tone	Sets an entry tone sound when a participant enters a conference.
Exit Tone	Sets an exit tone sound when a participant leaves a conference.
End Time Alert Tone	<p>Sets an alert tone to play into MCU-hosted conferences indicating that the conference is scheduled to end soon. Set the End Time Alert (minutes) field to configure when the tone should be played into the conference.</p> <p>Note</p> <p>This feature is not related to the system-based Conference Time Warning feature.</p>
End Time Alert (mins)	Specifies the number of minutes before the conference end that the End Time Alert Tone should sound.

Field	Description
Video Algorithm	<p>Sets the compression algorithm that the MCU uses to process video. Possible values include:</p> <ul style="list-style-type: none"> • Auto • H261. An ITU standard designed for two-way communication over ISDN lines and supports data rates which are multiples of 64Kbit/s. H.261 supports CIF and QCIF resolutions. • H263. Based on H.261 with enhancements that improve video quality over modems. It supports CIF, QCIF, SQCIF, 4CIF and 16CIF resolutions. • H264 <p>The default is Auto.</p> <p>Note</p> <p>Selecting a video algorithm doesn't guarantee that it will be chosen for a conference since the MCU device may negotiate a different algorithm with the endpoints, depending on the endpoint's capabilities.</p>
People + Content	<p>Enable this setting when you have equipment that supports the display of people and content. Sets the format type of the content. Possible values include:</p> <ul style="list-style-type: none"> • None • People+Content (H.239) • People and Content V0. To show both the presenter and the content on a single display using HDX-Series products. • Polycom Visual Concert PC. To show live PC content using standard ViewStation® systems • Polycom Visual Concert FX. To integrate a laptop with graphics into a video call using ViewStation® products • DuoVideo <p>None is the default.</p> <p>Note</p> <p>The MGC requires that conferences with People+Content use a minimum speed of 192 K.</p>
Talk Hold Time (secs)	<p>Indicates the minimum period that a participant has to speak to become the main speaker. During this period, no other participant may become the main speaker. The range is from 1.5 seconds to 10 seconds, in increments of 0.01 seconds.</p>

Field	Description
T120 Rate	<p>Determines whether T.120 is enabled, and if so, the default transfer rate. Enable this setting when you have equipment that supports T.120 display of data. Options are: 6.4, 14.4, 16, 22.4, 24, 30.4, 32, 38.4, 40, 46.4, 54.4, and 62.4.</p> <p>Note</p> <p>Because this setting uses resources on the MCU device, it is recommended that you select None.</p>
Audio Algorithm	<p>Sets the compression algorithm that the MGC uses to process audio.</p> <p>The default is Auto.</p> <p>Note</p> <p>Selecting a certain video/audio algorithm doesn't guarantee that it will be chosen for a conference since an MGC device may negotiate a different algorithm with the endpoints, depending on the endpoint's capabilities.</p>
Audio Mix Depth (sites)	<p>Sets the number of participants with the loudest voices who can speak at once during a conference. If additional participants speak, their comments are not heard.</p>
Conference on Port	<p>When selected, this option conserves bandwidth and ports by putting all participants on a single port. When Conference on Port is enabled, the Video Mode must be set to one of the Continuous Presence layouts.</p>
RMX General Settings > RMX Profile Settings	
Use existing profile	<p>Select to use an existing RMX profile.</p> <p>Clear to set all of the RMX profile settings here in the conference template. This method ensures that the RMX profile settings are the way you want them and avoids maintaining identical profiles on all RMX systems.</p> <p>Note</p> <p>With this option selected, conferences fail if they land on an RMX device and a valid RMX profile is not specified below.</p>
RMX profile name	<p>Identifies the RMX profile for the conference, if the conference is hosted on an RMX system.</p> <p>Enter the RMX profile routing name, which is generally (but not always) the same as the profile name as specified in the RMX platform.</p>

Field	Description
RMX General Settings > Conference Settings	
Video switching (VSW)	<p>In Video Switching mode, all participants see the same video picture (full screen). The current speaker is displayed in full screen on all the participants' endpoints, while the speaker sees the previous speaker. Switching between participants is voice-activated; whenever a participant starts to speak, he or she becomes the conference speaker and is viewed on all screens.</p> <p>When selected, the conference is of ultra-high quality video resolution, in a special conferencing mode which implies that all participants must connect at the same line rate and use HD video.</p> <p>This feature utilizes the resources more wisely and efficiently by:</p> <ul style="list-style-type: none"> • Saving utilization of video ports (1 port per participant as opposed to 4 ports in CP mode). • Video display is in full screen mode only. <p>Drawbacks of this feature are that all participants must connect at the same line rate, (for example, HD), and all participants with endpoints not supporting HD will connect as secondary (audio only).</p> <p>Video layout changes are not enabled during a conference. If HD 1080p is selected, endpoints that do not support HD 1080p resolution are connected as secondary (audio only) participants.</p> <p>Note:</p> <ul style="list-style-type: none"> • This option is not available if MGC is selected as a Supported MCU (General Settings). • Video Switching conferencing mode is unavailable to ISDN participants.
Resolution	<p>Possible values include:</p> <ul style="list-style-type: none"> • H.264 SD 30(v7 with MPM+ or MPMx) • H.264 720p60(v7 with MPM+ or MPMx) • H.264 720p30 • H.264 1080p30(MPM+ or MPMx)
RMX General Settings > Advanced Settings	
Auto redialing	<p>Instructs the Polycom RMX to automatically redial IP and SIP participants that have been abnormally disconnected from the conference.</p> <ul style="list-style-type: none"> • The RMX will not redial an endpoint that has been disconnected from the conference by the participant. • The RMX will not redial an endpoint that has been disconnected or deleted from the conference by an operator or administrator.

Field	Description
Encryption	Activate encryption for the conference
LPR	<p>Activate lost packet recovery (LPR) for the conference.</p> <p>Note:</p> <p>LPR can be enabled for VSW conferences, but H.320 and SIP participants will not be able to connect.</p>
Auto terminate	<p>When selected (default), the conference automatically ends when the termination conditions are met:</p> <ul style="list-style-type: none"> • Before first joins — No participant has connected to a conference during the n minutes after it started. Default idle time is 10 minutes. • At the end - After last participant quits — All the participants have disconnected from the conference and the conference is idle (empty) for the predefined time period. Default idle time is 1 minute. • At the end - When last participant remains — Only one participant is still connected to the conference for the predefined time period (excluding the recording link which is not considered a participant when this option is selected). This option should be selected when defining a profile that will be used for Gateway Calls and you want to ensure that the call is automatically terminated when only one participant is connected. Default idle time is 1 minute.
RMX Video Quality > People Video Definition	
Video quality	<p>Optimizes the video quality based on the amount of movement contained in the conference video. Possible values include:</p> <ul style="list-style-type: none"> • Motion—Provides a higher frame rate without increased resolution. • Sharpness—Provides a higher video resolution and requires more system resources.
Max resolution (v7)	<p>Depending on whether MPM+ or MPMx cards are installed, the possible values include:</p> <ul style="list-style-type: none"> • Auto • CIF • HD 1080 • HD 720 • SD

Field	Description
Video clarity (MPM+ and MPMx only)	<p>Applies video enhancing algorithms to incoming video streams of resolutions up to and including SD. Clearer images with sharper edges and higher contrast are sent back to all endpoints at the highest possible resolution supported by each endpoint.</p> <p>This option is not available if you select any of the following:</p> <ul style="list-style-type: none"> • Motion option for Video quality • Video switching (VSW) option (RMX General Settings)
Auto brightness (v7)	<p>Detects and automatically adjusts the brightness of video windows that are dimmer than other video windows in the conference layout.</p> <p>This option is not available if you set Telepresence mode to On (RMX Video Settings).</p>
RMX Video Quality > Content Video Definition	
Content settings	<p>Select the transmission mode for the content channel:</p> <ul style="list-style-type: none"> • Graphics — Basic mode, intended for normal graphics. • Hi-resolution graphics — Higher bit rate intended for high resolution graphic display. • Live video — Content channel displays live video. Selection of a higher bit rate for the content results in a lower bit rate for the people channel.
Content protocol	<p>The possible values are:</p> <ul style="list-style-type: none"> • H.263 — Content is shared using H.263 even if some endpoints have H.264 capability. • Up to H.264 — H.264 is the default content sharing algorithm. When selected: Content is shared using H.264 if all endpoints have H.264 capability. Content is shared using H.263 if all endpoints do not have H.264 capability. Endpoints that do not have at least H.263 capability can connect to the conference but cannot share content.

Field	Description
RMX Video Settings	
Send content to legacy endpoints (MPM+ and MPMx only)	<p>Content can be sent to H.323/ SIP/ISDN endpoints that do not support H.239 content (legacy endpoints) over the video (people) channel.</p> <p>This option is not available if you select any of any of the following:</p> <ul style="list-style-type: none"> • Video switching (VSW) option (RMX General Settings) • Same layout option <p>Notes:</p> <p>When enabled, additional video resources are allocated to the conference.</p>
Same layout	<p>Select this option to force the selected layout on all participants in a conference. Displays the same video stream to all participants and personal selection of the video layout is disabled. If participants are forced to a video layout window, they can see themselves.</p> <p>This option is not available if you select any of the following:</p> <ul style="list-style-type: none"> • MGC as a Supported MCU (General Settings) • Video switching (VSW) option (RMX General Settings) • Telepresence mode is On (RMX Video Settings)
Auto layout	<p>Select this option to have the system automatically select the conference layout based on the number of participants currently connected to the conference. When a new video participant connects or disconnects, the conference layout automatically changes to reflect the new number of video participants.</p> <p>Clear this option to manually select a layout for the conference using the Video Mode options.</p> <p>This option is not available if you select any of any of the following:</p> <ul style="list-style-type: none"> • MGC as a Supported MCU (General Settings) • Video switching (VSW) option (RMX General Settings) • Lecture View Switching option (Common Settings) • Telepresence mode is On (RMX Video Settings)

Field	Description
Telepresence mode (v6)	<p>The possible values are:</p> <ul style="list-style-type: none"> Auto (Default) - If any ITP (Immersive Telepresence) endpoints are detected, ITP features are applied to the conference video for all participants. The ITP features are dynamic. If all ITP endpoints disconnect from the conference, normal conference video resumes for all participants. ITP features resume for all participants if an ITP endpoint reconnects to the conference. On - ITP features are applied to the conference video for all participants regardless of whether there are ITP endpoints connected. Off - Normal conference video. <p>Note:</p> <ul style="list-style-type: none"> This field is enabled only if the RMX system is licensed for Telepresence Mode. This option is not available if MGC is selected as a Supported MCU (General Settings).
Telepresence layout mode (v6)	<p>Enables VNOC operators and Polycom Multi Layout Applications to retrieve Telepresence Layout Mode information from the RMX.</p> <p>The possible values include:</p> <ul style="list-style-type: none"> Manual Continuous Presence - Room continuous presence (default) Room Switch - Voice activated room switching <p>This option is not available if MGC is selected as a Supported MCU (General Settings).</p>
RMX Audio Settings	
Echo suppression	(Supported only with MPM+ or MPMx cards.) Enables an algorithm to search for and detect sounds outside the normal range of human speech (such as echo) and automatically mute them when detected.
Keyboard noise suppression	(Supported only with MPM+ or MPMx cards.) Enables an algorithm to search for and detect keyboard noises and automatically mute them when detected.
Audio clarity (v7)	<p>(Supported only with MPM+ or MPMx cards.) Improves received audio from participants connected via low audio bandwidth connections, by stretching the fidelity of the narrowband telephone connection to improve call clarity.</p> <p>The enhancement is applied to the following low bandwidth (8kHz) audio algorithms: G.729a and G.711.</p>

Field	Description
RMX Skins	<p>Select the skin you want. Skins modify the background and frames. With the top two skin options, the frames fill the screen with their borders touching.</p> <p>These options are not available if you select any of the following:</p> <ul style="list-style-type: none"> • Video switching (VSW) option (RMX General Settings) • Telepresence mode is On (RMX Video Settings)
RMX Conference IVR	
Override default conference IVR service	Select to override the default conference Interactive Voice Response (IVR).
Conference IVR service	If you selected the override option above, enter the name of the conference IVR service you want to use. All RMX systems that could be used must have the same conference IVR service set up.
Conference requires chairperson	<p>Select this option to require that a video chairperson control the conference from his or her video endpoint system.</p> <p>When this option is implemented, the system will assign a 15-digit password that the conference chairperson must enter to control the conference. The conference scheduler can change this system-assigned password to any 15-digit number.</p> <p>In this case:</p> <ul style="list-style-type: none"> • The video chairperson must have a video endpoint system. • The conference requires an MCU. • All conference participants remain in the waiting room and cannot join the conference until the conference chairperson enters the conference. <p>H.243 chair control allows an endpoint to control the conference using the H.243 chair control feature. The chairperson can disconnect participants, force the use of a continuous presence video layout, and terminate the conference.</p> <p>H.243 cascade control allows the MGC-50 or MGC-100 to support a cascading configuration of conferences with the capabilities of H.243.</p> <p>Note</p> <ul style="list-style-type: none"> • Set in the RMX profile for RMX 2000/4000 devices • The RMX 1000 system does not support the Chairperson feature.

Field	Description
RMX Recording	
Enable recording	Enables the recording settings. If no Recording links are found, an error message is displayed.
Record conference	The possible values are: <ul style="list-style-type: none"> • Immediately – Conference recording is automatically started upon connection of the first participant. • Upon request – The operator or chairperson must initiate the recording (manual).
Recording link (v7)	Enter the name of the Recording link you want to use. The recording link defines the connection between the conference and the recording system to be used for conference recording. Recording links defined on the RMX can be given a descriptive name and can be associated with a Virtual Recording Room (VRR) saved on the Polycom® RSS™ 4000 Version 6.0 Recording and Streaming Server (RSS). All RMX systems that could be used must have the same recording link set up.
Audio only	Records only the audio channel of the conference.
Indication of recording	Displays a recording icon to all conference participants informing them that the conference is being recorded. The recording icon is replaced by a paused icon when conference recording is paused.

Polycom CMA system has a **Default Template**. Administrators with **Conference Setup** permissions can edit the **Default Template** and create additional templates with different settings.

When scheduling a conference, the **Default Template**, which is available to all users, is selected by default. Schedulers can select a different conference template from the list of templates an administrator has made available to them. Users with advanced scheduling permissions can edit the template settings for a specific scheduled conference. These changes apply only to the specified conference.

Use these best practices when working with conference templates.

- For the **Default Template**, select settings that are the lowest common values for all device types. This ensures that all conferences scheduled with the **Default Template** can successfully launch on whatever devices the system has available at the time.
- The template names **Default Template** and **Default Audio Templates** are stored in the system database and their names are not localized into other languages. If you wish to localized their names into your language, edit the templates and enter new names for them.

- When creating new templates, give them meaningful purposes and names so that your users can easily identify the differences between template choices. For example, identify templates according to maximum bit rate, specific features implemented by the template (for example, Lecture Mode or Chairperson Control), and/or supported MCU type (MGC or RMX).
- In a mixed-MCU environment, consider the advantages and disadvantages of creating one or more conference templates for each MCU type. This ensures that the system can select a specific type of MCU and can implement the chosen conference settings.
- Remember that using an existing RMX profile will override settings specified when scheduling a conference through the Polycom CMA system. To ensure consistent and expected behavior, make sure to synchronize and lock down RMX profiles and Polycom CMA system conference templates.



Note

Polycom CMA systems do not support scheduling of third-party MCUs. Template settings apply only to the MGC or RMX devices.

Conference Settings

Conference settings apply to all conferences scheduled using the Polycom CMA system. These settings include:

Field	Description
Conference Time Warning	<p>Specifies whether or not the Polycom CMA system sends a message to video endpoints in a conference to warn the endpoint users that their conference is scheduled to end soon. The system sends the message 15 minutes and 5 minutes before the conference is scheduled to end.</p> <p>To support this feature, the video endpoint system must be capable of receiving a system Send Message action.</p> <p>By default, Conference Time Warning is enabled.</p> <p>Note</p> <p>This feature is not related to the MCU-based End Time Alert Tone feature.</p>
Automatically Include Conference Owner (Scheduler) in New Conferences	<p>Select this option when you wish the system to always include the person scheduling the conference as a conference participant. Do not select this option if your organization has assistants or operators schedule conferences for others.</p>

Field	Description
Allow overbooking of dial-in participants	Select this option to allow schedulers to schedule dial-in participants to dial into multiple conferences, but the system reserves resources for the participant for only the first scheduled conference
Conference and chairperson passcode length	<p>Designate the required length of the system-generated conference and chairperson passcodes. The acceptable length for both of these passcodes is 9 to 16 characters. By default, the required length for both of these passcodes is set to 15 characters.</p> <p>Note</p> <ul style="list-style-type: none">Depending on the system settings, the scheduler may be allowed to change the conference or chairperson passcode. However, the passcode length requirement still applies.If an administrator changes the passcode length here at the same time a scheduler edits the passcode settings for a scheduled conference, the scheduling operation may use either the old or the new length, depending on the exact timing.

Conference Setup Operations

This chapter includes information about conference options and tasks within the Polycom® Converged Management Application™ (CMA®) system. It includes these topics:

- [View the Conference Templates List](#)
- [Add a Conference Template](#)
- [Edit a Conference Template](#)
- [Delete a Conference Template](#)
- [Set Conference Settings](#)
- [Disable Conference Auto-Launch](#)
- [Disable Conference Time Warning](#)
- [Delete Customized Text in E-mail Notifications](#)
- [Overbooking Dial-in Participants](#)

View the Conference Templates List


To view the Conference Template list

- Go to **Admin > Conference Templates**.

The **Conference Templates** list appears.

Add a Conference Template

To add a conference template

- 1 Go to **Admin > Conference Templates**.
- 2 On the **Conference Templates** list, click **Add** .
- 3 Complete the **General Info** and **MCU Settings** sections of the **Add Conference Template** dialog box first. Your selection for **MCU Settings** affect your choices in the **Video Settings** section. For more information on the Add Conference Template dialog box, see [“Conference Templates”](#) on page 321.
- 4 Complete the **Video Settings** and **Conf Settings** sections of the **Add Conference Template** dialog box.
- 5 Click **OK**.

The new template appears in the **Conference Template** list.




Note

The CMA system does not validate the **Conference Template** settings. When you create a new conference template, you must make certain that the settings match the capabilities of the MCUs (MGC or RMX device) or endpoints.

Edit a Conference Template

To edit a conference template

- 1 Go to **Admin > Conference Templates**.
- 2 On the **Conference Templates** list, select the template of interest and click **Edit** .
- 3 Edit the **General Info**, **Video Settings**, **MCU Settings**, and **Conf Settings** sections of the **Edit Conference Template** dialog box as required.




Note

If you change the conference template **Speed** setting and there are scheduled conferences using that template, all endpoints in the scheduled conferences are reset to whichever is less: the new template **Speed** or the maximum speed that the endpoint supports.

- 4 Click **OK**.

Delete a Conference Template

To delete a conference template

- 1 Go to **Admin > Conference Templates**.
- 2 On the **Conference Templates** list, select the template of interest and click **Delete** .
- 3 Click **Yes** to confirm the deletion.

Set Conference Settings

To specify conference settings

- 1 Go to **Admin > Conference Settings**.
- 2 On the **Conference Settings** page, make the required selections.
[“Conference Settings”](#) on page 334.
- 3 Click **Update**.

Disable Conference Auto-Launch

To disable conference auto-launch

- 1 Go to **Admin > Conference Settings**.
- 2 In the **Conference Auto-Launch** section of the **Conference Settings** page, check the **Disabled** check box.
- 3 Click **Update**.

Disable Conference Time Warning

To disable the conference time warning

- 1 Go to **Admin > Conference Settings**.
- 2 In the **Conference Time Warning** section of the **Conference Settings** page, clear the **Enabled** check box.
- 3 Click **Update**.

Overbooking Dial-in Participants

In the CMA system, an administrator can configure the system to allow schedulers to overbook dial-in participants. In this case, dial-in participants can be scheduled to dial into multiple conferences, but the system reserves resources for the participant for only the first scheduled conference. Dial-out participants cannot be scheduled into multiple conferences.



Note

Schedulers can only overbook dial-in participants if they select a conference template that has the **Video Dial Option** set to **Dial-In Only**. A conference template that has the **Video Dial Option** set to **Dial In+Dial Out** will not work for this purpose.

To allow schedulers to overbook dial-in participants

- 1 Go to **Admin > Conference Settings**.
- 2 In the **Allow Overbooking of dial-in participants** section of the **Conference Settings** page, check the **Enabled** check box.
- 3 Click **Update**.

Add Customized Text to E-mail Notifications

To add customized text to all conferencing E-mail notifications

- 1 Go to **Admin > Server Settings > E-mail**.
- 2 In the **Text at the Beginning of the Reminder E-mail** section of the **E-mail** page, type in the introductory text you want to appear at the start of all conferencing E-mail notifications.

This text field is limited to 650 characters. The text you type here will appear in plain text just as you typed it.
- 3 In the **Text at the End of the Reminder E-mail** section of the **E-mail** page, type in the closing text you want to appear at the end of all conferencing E-mail notifications.

This text field is limited to 650 characters. The text you type here will appear in plain text just as you typed it.
- 4 Click **Update**.

Edit Customized Text in E-mail Notifications

To edit the customized text in all conferencing E-mail notifications

- 1 Go to **Admin > Server Settings > E-mail**.
- 2 To change the introductory text, replace the text in the **Text at the Beginning of the Reminder E-mail** section of the **E-mail** page with the new text you want to appear at the start of all conferencing E-mail notifications.

This text field is limited to 650 characters. The text you type here will appear in plain text just as you typed it.
- 3 To change the closing text, replace the text in the **Text at the End of the Reminder E-mail** section of the **E-mail** page with the new text you want to appear at the end of all conferencing E-mail notifications.

This text field is limited to 650 characters. The text you type here will appear in plain text just as you typed it.
- 4 Click **Update**.

Delete Customized Text in E-mail Notifications

To delete the customized text in all conferencing E-mail notifications

- 1 Go to **Admin > Server Settings > E-mail**.
- 2 To delete the introductory text, select the text in the **Text at the Beginning of the Reminder E-mail** section of the **E-mail** page and press **DELETE**.
- 3 To delete the closing text, select the text in the **Text at the End of the Reminder E-mail** section of the **E-mail** page and press **DELETE**.
- 4 Click **Update**.

Room Overview and Operations

This chapter describes how to set up rooms in the Polycom® Converged Management Application™ (CMA®) system. It includes these topics:

- [View the Rooms List](#)
- [Add a Local Room](#)
- [Add an Enterprise Room](#)
- [Edit a Room](#)
- [Delete a Room](#)

Local and Enterprise Meeting Rooms

The CMA system allows a user assigned the default **Administrator** role to manage local and enterprise meeting rooms and the endpoints associated with those meeting rooms.

Most often a CMA system is integrated with an enterprise directory to which rooms have been added. However, the CMA system also allows you to add local rooms (that is, rooms added manually to the system) and associate them with endpoints.

For dynamically managed endpoints associated with a room, you must also associate each room in the CMA system with a machine account. The machine account allows the room's endpoint to connect and authenticate with the CMA system for directory and dynamic management purposes without using the endpoint user's account. After you add a room, you can create the machine account and associate the room with the machine account. For more information, see "[Add Machine Accounts](#)" on page 460.

View the Rooms List

To view the Rooms list

- Go to **Admin > Rooms**.


The **Rooms** list appears. It can be filtered by **Site**.

Column	Description
Room Name	The unique and required name of the room.
Description	The optional description of the room.
Site	The location of the room as identified in the site topology.
Associated Endpoints	The primary endpoint associated with this room. A set of ellipses (...) indicates the room has more than one associated endpoint.

Add a Local Room

When you add a local room to a CMA system, you specify settings for it and associate one or more endpoints with it.

To add a local room

- 1 Go to **Admin > Rooms**.
 - 2 On the **Rooms** page, click **Add** .
- The **Add New Room** dialog box appears.
- 3 If you are logged into a domain other than the Local domain, click **Manually Define**.
 - 4 Complete the **General Info** and **Associated Devices** sections of the **Add New Room** dialog box. The following table shows the room information in the CMA system records.

Field	Description
General Info	
Room Name	The name of the room, which appears in the address book for associated endpoints.
Description	(Optional) A useful description (ASCII only) of the room.

Field	Description
Site	The site in which the room is located. Note Rooms and the endpoint associated with them must be assigned to the same site.
Email	(Optional) The E-mail address of the room administrator.
Associated Endpoints	
Available Endpoints	The list of unassigned endpoints that are managed by the CMA system.
Selected Endpoints	The list of endpoints assigned to the room. The endpoint at the top of the list is the primary endpoint. You can change the order of endpoint priority by selecting an endpoint and clicking Move Up or Move Down .

- 5 In the **Dial String Reservations** section, select the user's **Device** and enter the appropriate dial strings for **SIP URI**, **E164**, and **H323 ID**, then click **Apply**.

The dial strings appear in the list below.

If the user has multiple endpoints, enter the dial strings for one endpoint type at a time and click **Apply** each time.


- 6 Click **OK**.

The room is added to the CMA system. Note that the system does not distinguish between enterprise rooms and local rooms once they've been added to the system.

Add an Enterprise Room

If your CMA system is integrated with an enterprise directory, you can add a room from the enterprise directory to the CMA system.

To add an enterprise room

- 1 Go to **Admin > Rooms**.
- 2 On the **Rooms** list, click **Add Room** .

The **Add New Room** dialog box appears.

- 3 To find a room in the enterprise directory:
 - a In the **Search Value** field, type in the first few characters of the room name.


The system does a prefix search of the appropriate fields.
 - b Click **Search**.

A list of the enterprise users and rooms that meet the search criteria appears. If the search found more than 500 matching entries, only the first 500 are displayed.
 - c Select the room of interest and click **Define Details**.
- 4 Complete the **General Info**, **Associated Devices**, and **Dial String Reservations** sections of the **Add New Room** dialog box. For information on these fields, see [“Add a Local Room”](#) on page 344.
- 5 Click **OK**.

The room is added to the CMA system. Note that the system does not distinguish between enterprise rooms and local rooms once they’ve been added to the system.


Edit a Room

To edit a room

- 1 Go to **Admin > Rooms**.
- 2 In the **Rooms** list, select the room of interest and click **Edit** .
- 3 Edit the **General Info**, **Associated Devices**, and **Dial String Reservations** sections of the **Edit Room** dialog box. For information on these fields, see [“Add a Local Room”](#) on page 344.
- 4 Click **OK**.

Delete a Room

To delete a room

- 1 Go to **Admin > Rooms** .
- 2 In the **Rooms** list, select the room of interest and click **Delete**.
- 3 In the **Delete Room** dialog box, click **Yes**.

The room is deleted from the CMA system.

Area Overview and Operations

This chapter describes how to set up areas in the Polycom® Converged Management Application™ (CMA®) system. It includes these topics:

- [Areas Overview](#)
- [View Areas](#)
- [Create Area Administrator Role](#)
- [Enable, Configure, and Customize Areas](#)
- [Add Areas](#)
- [Assign Devices to Areas](#)
- [Associate Users with Areas](#)
- [Change Area Association for Users](#)
- [Delete an Area](#)

Areas Overview

Because the CMA system is a role-based system, users see only the pages and functions available to their roles and the permissions assigned to their user roles. However, users can perform those functions on any endpoint or network device defined to the system unless the **Areas** feature is implemented. By implementing areas, the CMA system administrator with **System Setup** permissions can limit access to endpoints and network devices to a specific set of administrators, operators, and schedulers.

How Areas Work

Areas add another dimension of permissions to scheduling, monitoring, and administration of endpoints and network devices. Besides the permissions enabled and disabled by roles and groups, the system now has a set of permissions enabled and disabled by areas.

Areas also limit access to directory entries. For example, a user associated with Area1 will not see a user associated with Area2 in the directory. However, the Area1 user can call the Area2 user with the correct H.323 address.

To implement areas, complete the following tasks

1 [Enable, Configure, and Customize Areas](#)

As a best practice, create an Area Administrator role. Assign that role to the people you want to administer devices in areas but not the CMA system itself.

2 [Enable, Configure, and Customize Areas](#)

A CMA system user with **System Setup** permissions can configure areas. When configuring areas, you can also change the term (both singular and plural) used to describe areas. For example, if you plan to limit users' access to devices based on their department, you may want to label this function Departments. If you plan to limit users' access to devices based on their line of business, you may want to label this function Line of Business.

3 [Add Areas](#)

A CMA system user with **System Setup** permissions can add areas. Adding areas includes naming the area, assigning devices to the area, and associating users with the area.

4 [Assign Devices to Areas](#)

A CMA system user with **Associate Devices to Areas** permissions can assign an area when adding or editing an endpoint or network device. To assign multiple devices to an area, you can use the **Assign Area** action on the **Monitor View** page. A device can only be assigned to one area. Only administrators associated with **All Areas** can assign a device with no area assignment to an area.

5 [Associate Users with Areas](#)

A CMA system user with **Assign CMA Users to Areas** permissions can associate users with one or more areas when adding or editing users. To associate multiple users with areas, you can use the **Assign Areas** action on the **User > Users** page. Users can be associated with multiple areas. Note that only users that have a CMA system role can be associated with areas.

Area Best Practices

Plan your area strategy with the following in mind:

- After you start assigning endpoints to areas, you must associate users with areas. The setting of **None** does not let users see endpoints assigned to an area.

- Endpoints and network devices can be assigned to only one area.
- Users can be associated with more than one area.
- Schedulers can only schedule endpoints assigned to the same area the scheduler is associated with.
- If you set up areas to correspond to sites, you must also set up site links between each site to permit calls between sites.

View Areas

You can view the list of existing areas from **Admin > Areas**. The following information is available.

Field	Description
Areas list	
Name	Meaningful name for the area.
Description	Description of the area.
Associated Devices	Number of devices assigned to the area.
Members	Number of users assigned to the area.
Summary	
Name	Name of the selected area.
Description	Description of the selected area.
Members	List of users associated with the selected area
User ID	Member's CMA system user ID.
First Name	Member's first name.
Last Name	Member's last name.
Associated Devices	List of endpoints and network devices assigned to the selected area.
Device ID	Device ID of the associated device.
Device Name	Device name of the associated device.
Site	Site of the associated device.

You may not see all areas that exist in the system. Only administrators that are associated with **All Areas** can see all the of areas in the system.

Create Area Administrator Role

As a best practice, create an area administrator role to separate CMA system administration from area administration.

To create an area administrator role

- 1 Go to **User > User Roles**.
- 2 On the **User Roles** page, click **Add**.
- 3 Complete the **Name** and **Description** fields of the **Add Role** dialog box and assign the desired permissions to the new role. At a minimum, add **Associate Devices to Area** permission to this role.
- 4 Click **Save**.

The new user role appears in the CMA system.

Enable, Configure, and Customize Areas

Before you can use areas, you must enable areas for endpoints and network devices. You can also change the term **Area** used in the CMA system interface to fit your use of areas.

To enable, configure, and customize the Areas function

- 1 Go to **Admin > Areas** and on the **Areas** page click **Configure Areas**.
- 2 In the **Configure Areas** dialog box, click **Enable Areas for endpoints and network devices**.
- 3 (Optional) To use a different term for the **Areas** function that is more meaningful to your business, enter the **Singular** and **Plural** term in the appropriate field. For example, Agency or Department.



Note

This configuration change will not take place until you restart the CMA system.

- 4 Click **Save Configuration**.
- 5 If you changed the **Area** term, go to **Admin > Dashboard** and click **Restart** to restart the CMA system.

After the system restarts, the **Areas** function will be renamed and enabled. By default, the CMA system maintains an **All** area, to which you, as the enabler of the function are assigned.

Add Areas

When you add areas, you can assign devices and users to the area.



Note

If the Areas option on your CMA system has been customized and renamed, the CMA system user interface will use that custom terminology.

To add areas

- 1 Go to **Admin > Areas** and click **Add**.
- 2 In the **Add an Area** dialog box, enter the **Area Name** and **Description**.
- 3 To associate devices with the area, click **Associate Devices**.
- 4 As needed, use the **Filter** to customize the device list.
- 5 Select the devices to be assign to the area and click the right arrow.
- 6 To assign users to the area, click **Assign Area Members**.
- 7 In the **Search Users** field, enter the name for the user of interest and press **Enter**.



Note

Searches for a user are case-insensitive, prefix searches of the **Username**, **First Name**, and **Last Name** fields.

- 8 Select the users to assign to the area and click the right arrow.
- 9 When complete, click **OK**.

Assign Devices to Areas

You can assign one or more unassociated devices to an existing area. Devices can only be associated with one area.



Notes

- After you assign devices with an area, only users associated with the same area or to **All Areas** can see the devices in the CMA system.
- The user setting of **None** does not let users see endpoints assigned to an area.

To assign devices to areas

- 1 Go to **Endpoint > Monitor View** or **Network Device > Monitor View**.

2 Click Associate Area.

The **Assign Area to Endpoints** or **Assign Area to Network Devices** dialog box appears with a list of endpoints or network devices.

3 Select the devices to assign to an area.**4 From the Assign Area drop-down, select the area to assign.****5 Click Assign Area.**

Associate Users with Areas

You can associate one or more users with an existing area. A user can be assigned to as many areas as needed.

**Note**

After you associate users with an area, they can only see devices assigned to the same area in the CMA system.

To associate users with areas**1 Go to Admin > Areas and click Manage Members.****2 In the Manage Area Members dialog box, enter the name for the user of interest in the Search Users field and press Enter.****Note**

Searches for a user are case-insensitive, prefix searches of the **Username**, **First Name**, and **Last Name** fields.

3 Select the users to assign to an area and click the right arrow.**4 Click Assign Areas.****5 Select one of the following options and click the right arrow.**

- **All Areas**—Gives the users access to all devices, regardless of the area the devices are assigned to.
- **Specific Areas**—Give the users access to only devices assigned to the areas selected below. Select one or more areas in the list below.

6 Click OK.

Change Area Association for Users

To remove area associations from users

- 1 Go to **Admin > Areas** and click **Manage Members**.
- 2 In the **Manage Members** dialog box, enter the name for the user of interest in the **Search Users** field and press **Enter**.



Note

Searches for a user are case-insensitive, prefix searches of the **Username**, **First Name**, and **Last Name** fields.

- 3 Select the user of interest and click the right arrow.
- 4 Click **Unassign Areas**.
- 5 Select the areas to unassign and click the right arrow.
- 6 Click **OK**.

Delete an Area

You can only delete areas that are not associated with devices or assigned members.

To delete an Area from the the Polycom CMA System

- 1 Go to **Admin > Areas** and on the **Areas** page select the area of interest.
- 2 Click **Edit**.
- 3 Click **Associate Devices** and move any devices out of the **Selected Devices** list.
- 4 Click **Assign Area Members** and move any devices out of the **Selected Area Members** list.
- 5 Click **OK**.
- 6 When the **Areas** page reappears, click **Delete**.
- 7 Click **Yes** to confirm the deletion.

Directory Operations

This chapter describes the Polycom® Converged Management Application™ (CMA®) enterprise directory integration and operations. It includes these topics:

- [Directory Management Overview](#)
- [Directory Management Supported Configurations](#)
- [Polycom CMA System and Windows Authentication](#)
- [Directory Management Operations](#)

Directory Management Overview

In a large organization, integrating your CMA system with Microsoft Active Directory greatly simplifies the task of managing conference system security. Directory management provides the following features.

- Single sign-on capability. Users get the benefits of pass-through authentication, allowing them to leverage their Active Directory user name and password to login to the Polycom CMA Desktop system. This happens without the user having to enter their credentials, creating seamless integration for logins.
- Single management environment. After the initial setup of the CMA system, adding groups into CMA system is no more complex than adding a group to a file share or database. Continue to manage your group memberships through Active Directory, then grant those groups rights within the CMA system.
- Allows you to continue leveraging the existing role-based security model that you have in place, though the CMA system only uses Universal groups.

Directory Management Supported Configurations

There are many possible configurations available within Microsoft Active Directory, some of which are not fully supported by the CMA system. This section describes the implications of different Microsoft Active Directory configurations for integrating with the CMA system.

Multiple Forests

Microsoft Active Directory may be set up in either a single-forest or multi-forest configuration. However, the CMA system requires that user accounts reside in a single forest.

Multiple Domains

Microsoft Active Directory forests may contain one or more domains. In either configuration, the directory must have a Global Catalog service. The CMA system can integrate to either single or multiple domains, so long as they reside in the same forest structure.

Microsoft Active Directory domains are organized into trees, each tree being a group of domains which share a consistent DNS namespace (ex: polycom.com and na.polycom.com would be in the same tree, while polycom.com and CMADevelopment.net would be separate trees, if they were in the same forest). The CMA system will integrate to all domains in a multi-tree forest.

Viable options:

- 1 Integrate to all domains of a multi-domain forest configuration.
- 2 Restrict to a single domain tree in a multi-domain forest through the use of LDAP Search baseDN criteria.

Groups

Microsoft Active Directory provides three group scopes: Universal, Global, and Domain Local. Both Global groups and Universal Groups are held on all Global Catalog servers in the forest. The CMA system supports only the Universal groups.

Microsoft Active Directory provides two group types: Security and Distribution. The CMA system supports either of these group types.



Note

An Active Directory forest with a functional level of Windows 2000 Mixed mode only supports Universal Distribution groups. Windows 2000 Native mode, Windows 2003 Mixed, and Windows 2003 forest functional levels support Universal Security and Distribution groups.

In addition to leveraging Active Directory Universal groups, the CMA system also has Local groups, which you can use to grant a standard set of rights to multiple users or groups. These CMA system Local groups can have as members, CMA system Local users, Active Directory users or Active Directory Universal groups. In this fashion, you can nest a variety of users and groups into a CMA system Local group and assign those users rights through their CMA system Local group membership, simplifying management of rights on the CMA system.

Users

The CMA system supports both local and enterprise user accounts. Local user accounts exist entirely on the CMA system. They can be created and managed whether or not the system is integrated to an enterprise directory. Enterprise user accounts exist in your enterprise Active Directory. The CMA system cannot create or manage Active Directory accounts, except to modify their privileges on the CMA system itself.

If simultaneously using local and enterprise accounts, it is important to avoid duplication of account data. For example, if your Active Directory has a user named John Doe with a username of jdoe, a local account for this user must possess a unique name, such as localjdoe or johndoetest. If duplicate user accounts exist in the same domain or across domains, the user associated with these accounts will not be able to log into a dynamically-managed endpoint.

The CMA system accesses the enterprise directory in a read-only mode. It does not create, modify, or delete Active Directory users or groups in any way.

Once you integrate with an enterprise directory, it's best to minimize your dependency on local users. A single local administrative user account must exist, and it should be used only when there is a problem connecting to the enterprise directory.

This configuration provides flexibility and varying security levels as follows:

- **Restricted access:** For security reasons, local user accounts do not have access to any data in Active Directory, though they can see the Active Directory users and groups as defined in the CMA system's security.
- **Administration:** Active Directory users and their Active Directory group memberships are managed through your Active Directory. CMA system local users are managed through the CMA system's web interface.

- Security: Local accounts have their own passwords, which are stored on the CMA system. Active Directory user accounts maintain the same users' Active Directory credentials and password complexity policies, which are validated by the domain controllers.

How Global Catalog Searches Work

When you integrate the CMA system with Active Directory, you can configure it to integrate in one of two ways:

- It can access a specific global catalog server by host name or IP address (not recommended, due to a lack of redundancy).

If you select this option, the domain name that you specify for the CMA system must match the DNS name suffix of the Global Catalog server (example: dc1.polycom.com configured as the Global Catalog, then you must enter polycom.com as the domain name of the CMA system server).

- It can auto-discover the server by querying the DNS for the closest Global Catalog server (strongly recommended).

If you select this option, you can specify any domain in the Active Directory forest in the Domain Name criteria for the CMA system server. The DNS server must contain Active Directory-specific entries.

It is recommended that you enter the forest root DNS domain name.

When configured to auto-discover the server, every time the CMA system needs to bind to a Global Catalog server for LDAP queries, the CMA system performs the following.

- Uses Microsoft's LDAP Ping mechanism to determine the site in which the system is located.
- Uses a DNS SRV record query to find a Global Catalog server within the same site.
- Connects to the Global Catalog on the domain controller and queries for the object in question and any relevant information (such as GUID, userID, name, phone number).

You can secure the connection between the CMA system and the Active Directory server's Global Catalog using **LDAP-S** (via outbound TCP/UDP port 3269) or **Start TLS** (via outbound 3268 TCP/UDP). To implement the secure connection, the appropriate ports must be open on any network equipment between the Global Catalog and the CMA system.

Accounts Required for the CMA System

CMA System Service Account

Before integrating the CMA system with an Active Directory forest, you must create a service account for it in Active Directory. This service account is a read-only user account that the CMA system uses to perform LDAP queries against your Active Directory Global Catalog.

CMA System Computer Account

The CMA system requires a computer account to enable secure channel communications with the Active Directory forest that is being leveraged for authentication. This account must be pre-created and the password set by an administrator from a Domain Controller.



Note

When setting up a redundant CMA system, the redundant servers use the same computer account to create their secure channel connection. The computer account name does not have to match the host name of your CMA system server.

Understanding Base DN

When the CMA system is integrated with an enterprise directory, the system uses the baseDN to determine domains and manage directory searches.

The **Base DN** field is where you specify the *distinguished name* (DN) of a subset of the Active Directory hierarchy (a domain, subset of domains, or organizational unit) to which you want to restrict the CMA system search. It acts like a filter.

By default, the **Base DN** field is empty. The first time you tell the system to connect to the enterprise directory server, leave the **Base DN** field empty. Once you have established a working connection with your Active Directory, then you enter a **Base DN**.

The following table illustrates some basic examples of Base DN filter expressions.

Search baseDN expression	Description
(ou=CMAGroups,dc=example,dc=com)	Include only groups and users which reside within the CMAGroups OU in the example.com domain.
(dc=example,dc=com)	Include only groups and users which reside within the example.com domain or domain tree.

Expressions in the Base DN and exclusion filter fields must be formatted according to RFC-4514, section 2.4.

Some special characters are allowed in the **BaseDN** field. They include:

Character	Character Name
" % "	Percent
" "	Space
" " "	Double quote
" ? "	Question mark
" { "	Open brace
" } "	Close brace
" ^ "	Caret
" ~ "	Tilde
" ["	Open bracket
"] "	Close bracket
" ' "	Single quote
" & "	Ampersand
" "	Pipe or bar

The special characters that are not allowed in the **Base DN** field without the special escape character (backslash, \) are:

Character	Character Name
" \ "	Backslash
" = "	Equal
" , "	Comma
" # "	Pound
" + "	Plus
" ; "	Semicolon
" < "	Less than
" > "	Greater than

Therefore, to use these character as part of a name, they must be preceded in the **Base DN** field by a backslash. For example, the baseDN of an ou named "tom, ann, bob" in the "myteam.example.com" domain must be entered as:

```
ou=tom\,ann\,bob\ dc=my team,dc=example,dc=com
```

Or the baseDN of an ou named "#+,=<>\ " in the "mydomain.example.com" domain must be entered as

```
ou=#\+,\,=\<>\|\| ,dc=mydomain,dc=example,dc=com
```

Note that this applies only to attribute values, not the *ou=* or *dc=* structure.

Understanding Exclusion Filters

Using LDAP exclusion filters, you can exclude objects in your directory based on a wide variety of criteria within your Active Directory environment. Any LDAP filters that you create must follow the LDAP standard and reference the LDAP display name of the attributes against which you are filtering.

The following table illustrates some basic examples of exclusion filter expressions.

Search baseDN expression	Description
Memberof=cn=Restricted Group,OU=users,dc=example,dc=com	Excludes all users who are members of "Restricted Group" within the Users OU in the example.com domain.
!(Memberof=cn=Video Users,OU=Users,dc=example,dc=com)	Includes only groups and users within the Video Users group in the Users OU in the example.com domain.

Creating exclusion filters can impact the performance of your LDAP queries. As a best practice, use indexed attributes and do not use medial searches when implementing exclusion filters. For more information, see [Creating More Efficient Microsoft Active Directory-Enabled Applications](#).

The following table illustrates some more advanced examples of exclusion filter expressions.

Search baseDN expression	Description
!((memberof=CN=Sales,DC=europe,DC=example,DC=com) (memberof=CN=IT,DC=europe,DC=example,DC=com))	Includes only users that are members of the 'Sales' or 'IT' Groups in the domain europe.example.com. Notes: <ul style="list-style-type: none"> The expression should be in continuous line with no carriage returns or extra spaces (not possible in this document's format). By excluding an entity, we implicitly mean to include all other entities. Conversely, by including an entity, we are implicitly excluding all other entities. Hence, this exclusion filter will suffice for a case where, for example, the administrator wants to include Sales and IT but exclude Human Resources, Engineering, etc., within the specified domain.
&(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840.113556.1.4.803:=2)	Excludes all users who are disabled. Note this is using a different but valid notation.

Polycom CMA System and Windows Authentication

To allow Microsoft Active Directory users with dynamically-managed endpoints to securely log into their endpoint without typing in their network credentials, the CMA system must be integrated with an Active Directory server and trusted by Active Directory.

When the CMA system starts up, it performs the following actions.

- Uses Microsoft's LDAP ping mechanism to determine the site in which the system is located.
- Uses a DNS SRV record query to find a domain controller within the same site.

When an Active Directory user attempts to log into the CMA system, it authenticates the user by connecting to the domain controller that it is connected to and passes the user's credentials using NTLMv2. The credentials are seamlessly passed to the CMA system utilizing a secure channel connection from the user's workstation, using the credentials with which they logged into the workstation.

**Note**

Because the CMA system uses NTLMv2, the password is not stored within and the CMA system never receives the user's password.

Some important notes about the CMA system Active Directory integration:

- The CMA system is not joined to the domain. Other computers on the network cannot browse its file system and it cannot be managed remotely by existing IT mechanisms such as SMS.
- The CMA system does not modify the Active Directory in any way.
- The CMA system can auto-discover the closest logical domain controller and Active Directory servers, but to do this the network DNS server must have a DNS SRV record for these servers. Once the domain controller's hostname and IP address have a record on the DNS, the CMA system can auto-discover the IP address of the domain controller. If your Active Directory does not publish the domain controller's hostname and IP address to the network DNS, you must edit the file to include it.
- The CMA system requires that you enable **Digitally sign communications** on the Active Directory server.

Directory Management Operations

This section describes the directory management operations. It includes these topics:

- [Integrate with Enterprise Directory Server Option](#)
- [Allow Delegated Authentication to Enterprise Directory Server](#)
- [Remove or Include Dynamically-Managed Endpoints in the Global Address Book](#)

Integrate with Enterprise Directory Server Option

The process of integrating with an enterprise directory server, involves these steps:

- [Create the Polycom CMA System Service Account](#)
- [Create the Polycom CMA System Computer Account](#)
- [Enable Integration with the Enterprise Directory Server](#)

Enabling the **Integrate with Enterprise Directory Server** option allows CMA system users who are included in the Active Directory to log into the CMA system interface using their network credentials.

Enabling the **Integrate with Enterprise Directory Server** option also allows endpoint users to select conference participants and rooms from the enterprise directory. Because endpoint connections to LDAP use the endpoint user's credentials, the Active Directory access control lists identify which endpoint users and rooms each user can see.

**Note**

The CMA system supports only the Microsoft Active Directory for its enterprise directory.

In addition, administrative users can:

- View some enterprise user and group information
- Import enterprise groups into the CMA system
- Assign roles to users in different enterprise groups
- Identify enterprise resources, such as rooms, so that they can be treated as resources in the CMA system

**Note**

To allow endpoint users to use NTLM Single Sign On technology to connect to the CMA system and access services such as automatic provisioning, automatic software update, and presence, see [“Allow Delegated Authentication to Enterprise Directory Server”](#) on page 367.

For more information about Active Directory and LDAP, see [MS Strategy for Lightweight Directory Access Protocol \(LDAP\)](#).

Create the Polycom CMA System Service Account

To create the CMA system service account

- 1 On the Active Directory server, open the **Active Directory Users and Computers** module (**Start > Programs > Administrative Tools > Active Directory Users and Computers**).
- 2 Click the node for your domain and then right-click the OU folder in which you want to add a user account and select **New > User**.
- 3 At a minimum, in the **First name**, **Full name**, and **User logon name** fields, type *cmaservice* or an appropriate name for your environment and click **Next**.
- 4 In the **Password** and **Confirm Password** fields, type a password for the service account to use during initial integration. This is the password you must enter on the CMA system **Enterprise Server** page.

- 5 Select the **Password never expires** option, unselect the **User cannot change password** option, click **Next** and then **Finish**.



Notes

- You can reset the password for this account manually, but to do so you must change it in Active Directory first and then update the CMA system LDAP Server page.
- The service account requires the rights to read all properties on all users and groups that will be used in the CMA system. Without these permissions, it may not function properly.

Create the Polycom CMA System Computer Account

To create the CMA System computer account

- 1 On the Microsoft Active Directory system, open the **Active Directory Users and Computers** module (**Start > Programs > Administrative Tools > Active Directory Users and Computers**).
- 2 Select the node for your domain, right-click the OU folder in which to add the computer account and then select **New > Computer**.
- 3 In the **Computer name** field, type *PolycomCMA* or an appropriate name for your environment and then click **Next** and **Finish** (or simply click **OK** depending on your version of Active Directory).
- 4 Ensure that the **Active Directory Users and Computers** console will show all available computer options necessary for the remaining steps by enabling **View > Advanced Features**.
- 5 Right-click the computer account, select **Properties**, and then select the **Security** tab.
- 6 In the **Group or user names** section of the Security tab, select the **SELF** object.
- 7 In the **Permissions for SELF** section, select **Change password**, and then click **OK**.
- 8 Login to the domain controller where the computer account was created and set the password using the following command:

```
net user <computername>$ <password>
```

For example: `net user polycomcma$ p@ssw0rd`



Notes

- Performing the net user command on any machine other than a domain controller will not assign the computer account password for the CMA system computer account.
- At initial integration, the CMA System will change its Computer Account password to a random 120 character string including special characters. This password will also be changed, to a new randomly generated password, every time the CMA System is rebooted, or every week if no reboots are performed. Because this is a Computer account, resetting the password to a known value requires use of net user commands on an Active Directory Domain Controller.

Enable Integration with the Enterprise Directory Server

To integrate the CMA system to an enterprise directory server

- 1 Go to **Admin > Directories > Enterprise Directory**.
- 2 On the **Enterprise Directory** page, select **Integrate with Enterprise Directory Server**.
- 3 To have the system auto-discover the server by querying DNS, enable **Auto-discover** in the **Enterprise Directory Server DNS Name** section; otherwise, enter the **DNS Name** for the enterprise directory server.
- 4 As needed, configure these settings.

Setting	Description
Domain\Enterprise Directory User ID	<p>Domain and Enterprise Directory User ID for an account that the CMA system can use to access the enterprise directory server and retrieve group, user, and room information. This is the account created “Create the Polycom CMA System Service Account” on page 364.</p> <p>This User ID must have read permissions so it can search the entire forest on the enterprise directory server.</p> <p>This User ID is automatically associated with the CMA system administrator role - by default it is the ONLY enterprise directory User ID with this role.</p>
Enterprise Directory User Password	The password for the enterprise directory user account

Setting	Description
Security Level	<p>The level of security on the connection between the CMA system and the enterprise directory server. Possible values include:</p> <ul style="list-style-type: none"> • Plain—No security on the connection • LDAPS—The connection is secured over outbound port 3269 using LDAP-S in a manner similar to <i>https</i>. If the “Domain Controller: LDAP Server signing requirements” setting on the Active Directory server is set to “Require Signing”, then you must use LDAPS to secure the connection. • StartTLS—The connection is secured over outbound port 3268 (the same port as Plain), but it then negotiates security once the socket is opened. Some LDAP servers reject any unsecured transactions, so the first command is the <i>StartTLS</i> negotiation command.
Ignore Disabled Enterprise Directory Users	Check this field to have the CMA system ignore disabled enterprise users in its queries.
Enterprise Directory Exclusion Filter	<p>If necessary and you understand the filter syntax, specify other types of user accounts to exclude. Don't edit these expressions unless you understand LDAP filter syntax.</p> <p>For more information, see “Understanding Exclusion Filters” on page 361.</p>
Enterprise Directory Search BaseDN	<p>If necessary and you understand the filter syntax, specify the top level of the enterprise directory tree (referred to as the base DN) to search. Don't edit these expressions unless you understand the filter syntax.</p> <p>For more information, see “Understanding Base DN” on page 359.</p>

- 5 If you also wish to implement single sign-on, see the following section [“Allow Delegated Authentication to Enterprise Directory Server”](#). Otherwise, click **Update**.

Allow Delegated Authentication to Enterprise Directory Server

The CMA system **Use Single Sign on (Integrated Windows Authentication)** option, allows endpoint users who are included in the enterprise directory to securely log into their dynamically-managed endpoint without typing in credentials.

**Note**

To allow CMA system users who enter their network usernames and passwords to log into the CMA system and select conference participants from your company's active directory, see ["Integrate with Enterprise Directory Server Option"](#) on page 363.

To delegate authentication to the enterprise directory server

- 1 Go to **Admin > Directories > Enterprise Directory**.
- 2 On the **Enterprise Directory** page, select **Allow delegated authentication to enterprise directory server**.
- 3 To have the system auto-discover the closest logical domain controller and enterprise directory servers, in the **Domain controller name** section enable **Auto-discover**; otherwise, enter the fully qualified hostname of the domain controller (for example, *dc1.mydomain.com*).

**Note**

To auto discover the domain controller and enterprise directory server, the network DNS server must have a DNS SRV record for these servers.

- 4 Enter the **Username** (*domain\<computer name>*) and **Password** and click **Update**.

Remove or Include Dynamically-Managed Endpoints in the Global Address Book

By default the CMA system includes dynamically-managed endpoints in the Global Address Book. However, you may not want to take advantage of this feature if you have legacy endpoints such as VSX, ViewStation, and FX endpoints. These endpoints may not be able to handle the increased size of the Global Address Book.

To remove enterprise users from the CMA system Global Address Book

- 1 Go to **Admin > Directories > Directory Setup**.
- 2 In the **Directory** page, clear **Include dynamically-managed devices in the Global Address Book**.
- 3 Click **Update**.

To include enterprise users in the CMA system Global Address Book

- 1 Go to **Admin > Directories > Directory Setup**.

- 2 In the **Directory** page, select **Include dynamically-managed devices in the Global Address Book**.
- 3 Click **Update**.

Remove or Include Guest Book Entries in the Directory

By default the CMA system includes Guest Book entries in the endpoint directory, regardless of whether the endpoint directory is the Global Address Book or the enterprise directory.

To remove Guest Book entries from the endpoint directory

- 1 Go to **Admin > Directories > Directory Setup**.
- 2 In the **Directory** page, clear **Show Guest Book entries in the Directory**.
- 3 Click **Update**.

To include Guest Book entries in the endpoint directory

- 1 Go to **Admin > Directories > Directory Setup**.
- 2 In the **Directory** page, select **Show Guest Book entries in the Directory**.
- 3 Click **Update**.

Support LifeSize Endpoints in Directories

You can include LifeSize endpoints in the endpoint directory by configuring your directory setup. When you do this, you also need to ensure that your LifeSize endpoint is configured to use the correct LDAP settings.

Complete the following steps:

- [“Modify Directory Listings”](#) on page 369
- [“Configure LDAP Settings”](#) on page 370

Modify Directory Listings

You need to allow your directory listings to include support for LifeSize endpoints.

To modify directory listings for LifeSize endpoint support

- 1 Go to **Admin > Directories > Directory Setup**.
- 2 In the **Directory Setup** page, mark the **Modify directory listings for LifeSize endpoint support** check box.

3 Click **Update**.

Configure LDAP Settings

In addition to configuring directory listing support in the directory set up, you need to also ensure that the LifeSize endpoint is configured to use the RealPresence CMA system's LDAP settings. You can provision these through a scheduled provisioning profile or configure them manually on the endpoint.

To add LDAP settings to a scheduled provisioning profile

- 1 Go to **Admin > Provisioning Profiles > Scheduled Provisioning Profiles**.
- 2 In the **Scheduled Provisioning Profiles** page, click **Add**.
- 3 In the **Add Profile** dialog box, select the **Endpoint Type** for the provisioning profile, enter a name for the profile, and click **Next**.
- 4 As needed, complete the various settings that you would like to provision for your LifeSize endpoint.

For more information about these fields, see [“Scheduled Provisioning of Polycom Endpoints”](#) on page 114.

- 5 For Directory support, select **the Directory > LDAP** page.
- 6 **On the Directory > LDAP page:**
 - a Mark the **Provision This Page** check box.
 - b In the **LDAP** field, select **Enabled** from the drop-down list.
 - » In the **LDAP Username** field, enter ***uid=ldapgab,ou=system***
 - » In the **LDAP Password** field, enter the password for the Polycom Global Address Book if you have one. If not, leave this field blank.
 - » In the **LDAP Base** field, enter ***DC=Polycom,dc=com***
- 7 Click **OK**.



If you manually enter the LDAP settings on the LifeSize endpoint, the value for the **LDAP Base** field needs to be the following:
OU=Endpoints,DC=Polycom,dc=com.

Directory Setup Operations

This chapter describes how to manage the Global Address Book in the Polycom® Converged Management Application™ (CMA®) system. It includes these topics:

- [View the Global Address Book](#)
- [Set or Change the GAB Password](#)

View the Global Address Book

The Polycom Global Address Book is a system managed endpoint directory that allows users with video endpoints to look up and call other users with video endpoints in their video communications network.

From a video endpoint system, users can locate other user's endpoints by name in the Global Address Book and initiate a call without knowledge of the other user's equipment. The CMA system will filter incompatible endpoints out of the Global Address Book (GAB) results so that the GAB presented to H.323-only endpoints will not include ISDN-only endpoints and the GAB presented to ISDN-only endpoints will not include H.323-only endpoints.



Note

GAB filtering applies only to Polycom endpoints. The GAB is not filtered on third-party endpoints.

For more information on the Global Address Book, see [“Endpoint Directory and Directory Settings”](#) on page 401.

To view the Global Address Book

- 1 Go to **Admin > Directories > Global Address Book**.
- 2 As needed, use the **Filter** to customize the **Global Address Book**. It can be filtered by **Endpoint Name** or **IP Address**.

The user information found in the **Global Address Book** includes:

Column	Description
Owner	The associated user or resource ID.
Name	The name of the registered endpoint.
GAB Display Name	The name of the registered endpoint as it will be displayed to other endpoint users. This display name is an ASCII only field.
Type	The type of endpoint.
IP Address	The IP address of the endpoint.
Phone Number	The phone number of the endpoint.
Alias	The alias associated with the endpoint.


Set or Change the GAB Password

You can require that endpoints be provisioned with a password in order to access the Global Address Book on the CMA system. To do so, set a Global Address Book password as described here. Use the same procedure to change the Global Address Book password.

Note that even if the Global Address Book is password protected, some third-party endpoints may not be required to provide a password because they are not directory-password aware. They have unrestricted access to the Global Address Book.

To provision this password to endpoints, see [“Add a Scheduled Provisioning Profile”](#) on page 186.

To set or change the password for the Global Address Book

- 1 Go to **Admin > Directories > Global Address Book**.
- 2 In the **Global Address Book**, click **Set GAB Password** .
- 3 In the **Set Client Password** dialog box, enter the **Old Password** and the **New Password**. (Note that the password fields are ASCII only.)
- 4 Confirm the new password and click **Save**.

Once you set this password, endpoints that are not provisioned with this password cannot access the Global Address Book on the CMA system.

Multiple Address Books

This chapter describes how to set up multiple address books in the Polycom® Converged Management Application™ (CMA®) system. It includes these topics:

- [Multiple Address Books Overview](#)
- [How Multiple Address Books Work](#)
- [View the Address Book List and Details](#)
- [Add an Address Book](#)
- [Edit an Address Book](#)
- [Assign Address Books to Groups](#)
- [Viewing the Address Book a User is Assigned To](#)
- [Delete an Address Book](#)
- [Change Address Book Priority](#)
- [Set the Default Address Book](#)
- [Copy an Address Book](#)

Multiple Address Books Overview

Users assigned the **Administrator** role can create multiple address books in the CMA system. Multiple address books are subsets of the Global Address Book (GAB) and let you manage which users (local and enterprise), endpoints, rooms, groups, and guests appear in each address book.

Multiple address books support both the GAB and LDAP protocols. Endpoints requesting directory information using either protocol receive either the default address book or the address book assigned to the user's group.

If you do not want to use multiple address books, you can leave the default address book set to **All Entries**. Using this default, all users will see all entries in the directory. Be sure that all groups are assigned either the **System Default** or **All Entries** option. **System Default** is the default group setting.

**Notes**

- Multiple Address Book functionality works in Maximum Security Mode based upon LDAP only.
- An endpoint must be associated with a User and the User must be in a Group in order to specify an address book.

How Multiple Address Books Work

Use address books to limit access to people and endpoints. For example, you can set up separate address books for each department in your organization. Each address book would include only CMA users in that department and only rooms in that department's location.

If the CMA system has the Areas feature enabled, you can only associate users and endpoints in the same Areas as you are in to address books.

Users not assigned the **Administrator** role will not be aware of address books. They will see only those users (local and enterprise directory), endpoints, rooms, groups, and guests in the same address book that the user is assigned to.

To implement multiple address books, complete the following tasks

1 [Add an Address Book](#)

CMA system users assigned the **Administrator** role can create address books and associate users (local and enterprise directory), endpoints, rooms, groups, and guests with one or more address books. This process controls where each entity appears as an address book entry.

2 [Assign Address Books to Groups](#)

CMA system users assigned the **Administrator** role can assign an address book to a group. A group can be assigned to only one address book. This process controls the address book that users and endpoints have access to.

3 [Change Address Book Priority](#)

CMA system users assigned the **Administrator** role can set the priority of address books. The priority affects which address book a user has access to. For example, if a user is a member of two different groups and each group is assigned a different address book, the user can access the address book that is higher in priority.

View the Address Book List and Details

To view the address book list and details

- 1 Go to **Admin > Directories > Address Books**.

The Address Book list appears, with details of the selected address book in the right pane.

Column	Description
Priority	The priority affects which address book a user sees. For example, if a user is a member of two different groups and each group is assigned a different address book, the user will see the address book that is higher in priority.
Address Books	Name of the address book.
Description	A brief description of the address book.

- 2 In the **Address Book Details** in the right pane, expand the tree to view the tiers along with users, endpoints, rooms, groups, and guests associated with the address book.

Add an Address Book

You can add many address books to the CMA system, and each address book can have up to 100 tiers.

Tiers are only meant to allow you to organize the address book contents. They will not be visible to endpoint users when they access the directory. Each tier can have up to three subtiers, and you can have address book entries at any tier level.

Associating users, endpoints, rooms, groups, and guests with an address book controls where these entities appear. For example, if you associate user A with address book A, the user will appear as an entry in address book A. You can associate any of these entities with more than one address book, and the entity will appear as entry in each address book.

Groups in the CMA system control the address book users, endpoints, and rooms have access to. To set which address book an entity has access to, see [“Assign Address Books to Groups”](#) on page 379.

To add an address book

- 1 Go to **Admin > Directories > Address Books**.
- 2 Click **Add**.

3 Complete the fields in the Add an Address Book dialog box.

Field	Description
Address Book Information	
Name	A meaningful name to identify this address book.
Description	A brief description of the address book.
Address Book Tiers	
New Tier	Select where you want to add a tier and click to add a new tier to the address book.
Edit Tier Name	Select a tier and click to change a tier name.
Delete	Select a tier and click to delete a tier.

4 To associate users with this address book, click **Associate Users**.

The **Address Book/Tier** column shows all of the address books the users appear in.

- a** Search for the users you want to associate. Use the **Filter** to customize the list.
- b** Select the users you want and click **Specify Tier**.
- c** Select the tier you want for the users and click **OK**.

5 To associate endpoints with this address book, click **Associate Endpoints**.

Only endpoints that are not associated with a CMA system user appear in the list.

- a** Use the **Filter** to customize the list.
The **Address Book/Tier** column shows all of the address books the endpoints appear in.
- b** Select the endpoints you want and click **Specify Tier**.
- c** Select the tier you want for the endpoints and click **OK**.

6 To associate rooms with this address book, click **Associate Rooms**.

The **Address Book/Tier** column shows all of the address books the rooms appear in.

- a** Use the **Filter** to customize the list.
- b** Select the rooms you want and click **Specify Tier**.
- c** Select the tier you want for the rooms and click **OK**.

- 7 To associate groups with this address book, click **Associate Groups**.
The **Address Book/Tier** column shows all of the address books the groups appear in.
 - a Use the **Filter** to customize the list.
 - b Select the groups you want and click **Specify Tier**.
 - c Select the tier you want for the groups and click **OK**.
- 8 To associate guests with this address book, click **Associate Guests**.
The **Address Book/Tier** column shows all of the address books the guests appear in.
 - a Use the **Filter** to customize the list.
 - b Select the guests you want and click **Specify Tier**.
 - c Select the tier you want for the guests and click **OK**.
- 9 Click **OK**.

Edit an Address Book

You can edit an address book to add or remove users, endpoints, rooms, groups, and guests.

You can find any of these entities that are not currently associated with an address book by selecting **Current Association** from any **Filter**, then selecting **Not Associated With An Address Book**.

If a group is set up with the **Enterprise Directory Viewable** option not selected, you can still add that group to an address book. The group itself will not appear as an entry in the address book, but the members of the group will.

To edit an address book

- 1 Go to **Admin > Directories > Address Books**.
- 2 Select an address book.
- 3 Click **Edit**.
- 4 Edit the fields in the Edit an Address Book dialog box.

Field	Description
Address Book Information	
Name	A meaningful name to identify this address book.
Description	A brief description of the address book.

Field	Description
Address Book Tiers	
New Tier	Select where you want to add a tier and click to add a new tier to the address book.
Edit Tier Name	Select a tier and click to change a tier name.
Delete	Select a tier and click to delete a tier.

- 5** To associate users with this address book, click **Associate Users**.

The **Address Book/Tier** column shows all of the address books the users appear in.

- a** Search for the users you want to associate. Use the **Filter** to customize the list.
- b** Select the users you want and click **Specify Tier**.
- c** Select the tier you want for the users and click **OK**.
- d** To delete a user from the address book, select the user and click **Delete**.

The user is removed from the address book, but remains in the CMA system.

- 6** To associate endpoints with this address book, click **Associate Endpoints**.

Only endpoints that are not associated with a CMA system user appear in the list.

The **Address Book/Tier** column shows all of the address books the endpoints appear in.

- a** Use the **Filter** to customize the list.
- b** Select the endpoints you want and click **Specify Tier**.
- c** Select the tier you want for the endpoints and click **OK**.
- d** To delete an endpoint from the address book, select the endpoint and click **Delete**.

The endpoint is removed from the address book, but remains in the CMA system.

- 7** To associate rooms with this address book, click **Associate Rooms**.

The **Address Book/Tier** column shows all of the address books the rooms appear in.

- a** Use the **Filter** to customize the list.
- b** Select the rooms you want and click **Specify Tier**.
- c** Select the tier you want for the rooms and click **OK**.

- d** To delete a room from the address book, select the room and click **Delete**.
The room is removed from the address book, but remains in the CMA system.
- 8** To associate groups with this address book, click **Associate Groups**.
The **Address Book/Tier** column shows all of the address books the groups appear in.
 - a** Use the **Filter** to customize the list.
 - b** Select the groups you want and click **Specify Tier**.
 - c** Select the tier you want for the groups and click **OK**.
 - d** To delete a group from the address book, select the group and click **Delete**.
The group is removed from the address book, but remains in the CMA system.
- 9** To associate guests with this address book, click **Associate Guests**.
The **Address Book/Tier** column shows all of the address books the guests appear in.
 - a** Use the **Filter** to customize the list.
 - b** Select the guests you want and click **Specify Tier**.
 - c** Select the tier you want for the guests and click **OK**.
 - d** To delete a guest from the address book, select the guest and click **Delete**.
The guest is removed from the address book, but remains in the CMA system.
- 10** Click **OK**.

Assign Address Books to Groups

You can assign an address book to a group, but you cannot assign address books directly to users. Group assignment controls to which address book users and endpoints have access. Each group can have just one address book assigned to it, but users can be in more than one group.

Address book priority affects which address book users and endpoints can access. For example, if a user is a member of two different groups and each group is assigned a different address book, the user will see the address book that is higher in priority. To change priority, see [“Change Address Book Priority”](#) on page 381.

To assign an address book to a group

- 1 Go to **User > Groups**.
- 2 Select the group you want to assign.
- 3 In the **Edit Local Group** dialog box, select address book you want from the **Assign Address Book** drop-down list.
- 4 Click **OK**.

Viewing the Address Book a User is Assigned To

You can see which address book a user is assigned to. The address book assignment controls the address book entries a user or endpoint can access.

To view the address book a user is assigned to

- 1 Go to **User > Users**.
- 2 Select the user you want.
- 3 Click **View Details**.
- 4 In the **View User** dialog box, click **Inherited Group Info**.
- 5 Click **OK**.

Delete an Address Book

You can delete an address book when it is no longer needed. Deleting an address book does not delete the users, endpoints, rooms, groups, or guests that were in the address from the CMA system.

Any entity that was assigned the deleted address book will have access to one of the following:

- Another address book if the entity is a member of another group that is assigned to an existing address book.
- The default address book.

To delete an address book

- 1 Go to **Admin > Directories > Address Books**.
- 2 Select the address book you want to delete.

3 Click **Delete**.

A confirmation message appears.

4 Click **Yes**.

Change Address Book Priority

You can change the priority of address books. The priority determines which address book a user sees. For example, if a user is a member of two different groups and each group is associated with a different address book, the user will see the address book that is higher in priority.

The **All Entries** address book always has the highest priority and **None** always has the lowest priority. If the address book for one of the groups the user belongs to is changed to **All Entries**, the user will see all entries regardless of the priority of the address book for the other group.

To change address book priority

1 Go to **Admin > Directories > Address Books**.

2 In the Priority column of an address book, enter the priority you want.

Use only whole numbers and only numbers that fall within the total count of address books. For example, if you have four address books, only 1 through 4 are valid priority values.

3 Click **Update Priority**.

The system changes the order of the address book list.

Set the Default Address Book

You can set the default address book. The default address book sets the address book all new users have access to if no address book is assigned through a group.

If you do not want to use multiple address books in the CMA system, leave the default address book set to **All Entries** (the default). Using this default, all users will be able to see all entries in the directory. Be sure that all groups are assigned either the **System Default** or **All Entries** option. **System Default** is the default group setting.

If you create multiple address books, you can change the default address book to one of the address books you created.

To set the default address book

- 1** Go to **Admin > Directories > Address Books**.
- 2** Click **Set Default**.
- 3** In the Default Address Book dialog box, select the option you want:
 - **All Entries** – Default setting. All users, endpoints, groups, rooms, and guests are in one address book and all have access to all address book entries.
 - **None** – No directory entries will be available.
 - **Specify** – Select the address book you want as the default.
- 4** Click **OK**.

Copy an Address Book

You can copy an existing address book as a shortcut to creating a new address book. The copy process can copy the entire address book or just the tier structure.

To copy an address book

- 1** Go to **Admin > Directories > Address Books**.
- 2** Select the address book you want to copy.
- 3** Click **Copy**.
- 4** In the **Copy AddressBook** dialog box, select the option you want:
 - **Entire AddressBook** – This option copies all of the tiers and the users, endpoints, rooms, groups, and guests that are associated with the address book to the new address book.
 - **Tiers only** – This option copies only the tier structure to the new address book.
- 5** Enter a meaningful **Name** and **Description**.
- 6** Click **OK**.

You can now edit the new address book to add or delete entries.

Polycom CMA System Setup Overview

This chapter provides an overview of the Polycom® Converged Management Application™ (CMA®) **System Setup** menu. It includes these topics:

- [Server Settings](#)
- [Polycom CMA System Licensing](#)
- [Polycom CMA System Site Topology and Dial Plan Set Up](#)
- [Polycom CMA System Gatekeeper Functionality](#)
- [Routing Mode](#)
- [Polycom CMA System Integration with Microsoft Outlook](#)
- [Polycom CMA System Integration with Microsoft Lync Server 2010 or Microsoft Office Communications Server 2007](#)
- [Endpoint Directory and Directory Settings](#)

Server Settings

Most of the selections in the **Server Settings** menu are entered during the CMA system First Time Setup process and do not change frequently. Use the **Server Settings** menu, when you do need to change them.

The **Server Settings** menu allows users with Administrator permissions to implement the CMA system configuration best suited for their corporate environment as identified in the solution design, site survey, and/or network design.

The **Server Settings** menu includes these items:

Selection	Description
Network	The basic network setting for the CMA system on your network.

Selection	Description
Gatekeeper Settings	<p>By default the CMA system is made the primary gatekeeper during the First Time Setup process. Use the Gatekeeper Settings option to modify the primary gatekeeper behavior or to add an alternate gatekeeper or neighboring gatekeepers.</p> <p>Gatekeeper Settings affect how devices register and calls are made in your video communications network. These settings allow you to:</p> <ul style="list-style-type: none"> Identify the gatekeeper with an identifier and description. Specify registration-related settings, including the default gatekeeper, which endpoints register, the registration refresh period, and the offline timeout. Set the maximum number of neighboring gatekeeper hop counts. Specify how to handle calls to and from unregistered endpoints.
Management and Security Settings	<p>Management Settings allow you to upgrade the CMA system software and enable auto discovery of endpoints.</p> <p>Security Settings allow you to implement HTTPS for the CMA system.</p>
Dial Plan Settings	<p>Edit the default CMA system Dial Plan and Site settings (which includes the definition of sites, site links, dial rules, services, and least-cost routing tables) to support your network topology and video call routing.</p>

Polycom CMA System Licensing

The seat capacity for a CMA 5000 system with the Maximum Security feature not enabled scales from 500 to 5,000 devices. The entry-level CMA 5000 system has a baseline capacity of 500 client access licenses. Additional licensing is offered in 100, 500, and 1000 license pack sizes.

The seat capacity for a CMA 4000 system with the Maximum Security feature not enabled scales from 200 to 400 devices. The entry-level CMA 4000 system has a baseline capacity of 200 client access licenses. Additional device licensing is offered in 100 license pack size.

The seat capacity for a CMA 5000 system with the Maximum Security feature enabled is fixed at 500 devices with no expansion available. A CMA 4000 cannot operate in Maximum Security mode.

Your system comes with a Default Trial key that is valid for 60 days after activating your system. With your system order, you will receive one License Certificate. You must activate the License Certificate to receive an activation key, which you then enter in the CMA system. When you enter this activation

key into the system, it overwrites the Default Trial key.

When applied to the system, an expansion license pack augments the device license count. For example, applying a 1000-device expansion license pack to a baseline CMA 5000 system will yield a total license count of 1500 concurrent licenses.

Where applicable, the number of concurrent calls supported by a CMA system is derived from the number of device licenses at a 3/10 ratio (calls/devices). For example, a system licensed for 5000 devices supports up to 1500 concurrent calls in routed mode and 3000 calls in direct mode.

Device licenses are consumed based on a 1:1 basis for any managed device (endpoints, MCU, GK, GW – including personal endpoints, IP blades, and more) that can be added to the system by any means, including the user interface, registration for management services, or registration for Global Address Book services.



Note

Device licenses are consumed by managed devices, not by users. You may add any number of local or enterprise users to the CMA system.

The CMA system has the following licensing packages:

- Base system license
- Base system license with Microsoft Outlook
- Base system license with IBM Lotus Notes
- Base system license with Microsoft Outlook and IBM Lotus Notes
- Redundant system licenses (primary and redundant licenses)
- Redundant system licenses with Microsoft Outlook
- Redundant system licenses with IBM Lotus Notes
- Redundant system licenses with Microsoft Outlook and IBM Lotus Notes

Licensing for the Polycom CMA Desktop client is included with the CMA system. When a Polycom CMA Desktop client is provisioned by the CMA system, it automatically consumes a license. That license is then reserved for that Polycom CMA Desktop client. However, you can configure the CMA system to automatically release a Polycom CMA Desktop client license after a set number of days of inactivity.

Licenses consumed by registered hardware devices are never automatically released. To release a license from a registered hardware device, an administrator must manually delete the device from the system.

Polycom CMA System Site Topology and Dial Plan Set Up

Site topology information describes your network and its interfaces to other networks, including the following elements:

- **Site** — A local area network (LAN) that generally corresponds with a geographic location such as an office or plant. A site contains one or more network subnets, so a device's IP address identifies the site to which it belongs.
- **Network clouds** — A Multiprotocol Label Switching (MPLS) network cloud defined in the site topology. An MPLS network is a private network that links multiple locations and uses label switching to tag packets with origin, destination, and quality of service (QoS) information.

Note that MPLS clouds are not associated with an IP address ranges, so they can be used to group multiple subnets. They could also represent a service provider.

While links to MPLS clouds have bandwidth and bit rate limitations, the cloud is infinite. In this way, clouds reflect the way in which businesses control bandwidth and bit rate.

- **Internet/VPN** — A entity that represents your network's connection to the public Internet.
- **Site link** — A network connection between two sites or between a site and an MPLS network cloud.
- **Site-to-site exclusion** — A site-to-site connection that the site topology doesn't permit an audio or video call to use.
- **Territory** — A grouping of one or more sites for which a CMA system is responsible.

The site topology you create within the CMA system should reflect your network design. Consider the following information and best practices when creating your site topology:

- If possible, connect all sites to an MPLS cloud. MPLS clouds are like corporate networks, used to connect multiple subnets in multiple sites, but all servicing a company.
- Avoid cross loops or multiple paths to a site; otherwise a call may have different paths to a single destination. The more cross, circular, and multi paths you have, the higher the number of calculations for a conference.
- Link sites that aren't connected to an MPLS cloud directly to another site that is connected to an MPLS cloud. Do not create orphan sites.
- Calls are routed through a bridge, so bandwidth and bit rate limits for the site and subnet apply to all calls made using that bridge.
- Reserve the Internet/VPN "site" for IP addresses that fall outside your private or corporate network (for example remote workers), because all calls routed to the Internet/VPN site will be routed through the site on your private or corporate network that has Internet access.

The CMA system site topology function uses a dynamic, embedded mapping tool that graphically displays the sites, clouds (network and Internet), and site links (site-to-site or site-to-cloud) in your network.



Within this global and graphical view of the video conferencing network, you can:

- Create and link up to 500 sites
- Zoom and pan to view specific network components
- View system and device alarms
- View the video network capacity for sites and site links as indicated by the color and shape of its icons.
- Filter the view by site name, territory name, IP address, network devices, and alerts

Sites List

The **Sites** page contains a list of the sites defined to the CMA system.

Use the commands in the **Actions** list to add a site, edit or delete existing sites, and see information about a site, including the number of devices of each type it contains.

The following table describes the fields in the **Sites** list.

Column	Description
Name	Name of the site.
Description	Description of the site.

Column	Description
Country Code	The country code for the country in which the site is located.
Area Code	The city or area code for the site. Do not include a leading zero. For example, the city code for Paris is 01; however, enter 1 in this field.
Max Bandwidth (Mbps)	The total bandwidth limit for audio and video calls.
Max Bit Rate (Kbps)	<p>The per-call bandwidth limit for audio and video calls.</p> <p>Note</p> <p>Bit rate is not the same as bandwidth. Since the bit rate applies in both directions and there is overhead, the actual bandwidth consumed is about 2.5 times the bit rate.</p>
Territory	The territory to which the site belongs, which determines the CMA system responsible for it.

Add/Edit Site Dialog Box

Use the **Add Site** dialog box to define a new site in the CMA system's site topology and specify which subnets are associated with it. Use the **Edit Site** dialog box to redefine information for an existing site.

The following table describes the fields in the **Add Site** and **Edit Site** dialog boxes.

Field	Description
General Info	
Site Name	A meaningful name for the site. The name can be up to 32 characters long, and may include spaces, dashes, and underscores.
Description	A brief description (ASCII only) of the site.
Override ITU Dialing Rules	Check this box to override the standard dial rules established by the International Telecommunications Union.
PBX Access Code	The access code required to enter the site's PBX system.
Country Code	The country code for the country in which the site is located.
Area Code	The city or area code for the site. Do not include a leading zero. For example, the city code for Paris is 01; however, enter 1 in this field.

Field	Description
# of Digits in Subscriber Number	The number of digits in a phone number. For example, in the United States, subscriber numbers may have seven digits or ten digits depending upon the region.
Default LCR Table	The default least-cost routing table (LCR) for this site. This LCR table is used for all calls originating from devices associated with this site. The default is None .
Assignment Method	<p>The ISDN number assignment method for the site. Possible values include:</p> <ul style="list-style-type: none"> • No Auto Assignment. Select this option when ISDN numbers are not assigned to IP devices. • DID (Direct Inward Dial). Select this option when you assign a range of phone numbers received from the telephone company service. • Gateway Extension Dialing. Select this option when you have a single gateway phone number and a range of extensions (E.164 aliases) that are internal to the company. In this case, calls go through a gateway. Endpoints are differentiated by the extension at the end of the dial string. <p>When a site is assigned an automatic assignment method, devices without an ISDN number are assigned one when they register. These numbers allow inbound calls to reach specific video endpoints. After an ISDN number is assigned to an endpoint, it is reserved for use as long as that endpoint remains registered with the CMA system.</p> <p>Note</p> <p>If you do not assign ISDN numbers automatically, you cannot call IP-only endpoints through an ISDN line.</p>
Territory	Assigns the site to a territory, and thus to a CMA system.
Location	Specify the geographic location of the site either by longitude+latitude or country+city.
ISDN Number Assignment— Assignment Method = DID (Direct Inward Dial)	
# Digits in Call Line Identifier	<p>Enter the number of digits in the Call Line Identifier (CLID), which is the dialed number. The maximum is 17.</p> <ul style="list-style-type: none"> • For example, in the United States, the number of digits in the CLID is often 7 for outside local calls, 4 for internal calls, or 11 for callers in a different area code. • This number indicates what part of the full dial string is sent to the gatekeeper for address resolution.

Field	Description
# Digits in Short Phone Number	<p>Enter the number of digits in the short form of the dialing number.</p> <ul style="list-style-type: none"> For example, in the United States, internal extensions are usually four or five digits. This number indicates what part of the dial string is sent to the gatekeeper for address resolution in gateway + extension dialing.
ISDN Number Range - Start	The starting ISDN number to assign automatically to IP devices.
ISDN Number Range - End	The ending ISDN number to assign automatically to IP devices.
ISDN Number Assignment— Assignment Method = Gateway Extension Dialing	
Gateway Phone Number	Phone number of the site gateway.
E164 Start	<ul style="list-style-type: none"> The starting number in a range of available extensions to assign automatically to IP devices. When a device without native ISDN registers, a number within the start and end range is assigned, so that the device can be called through an ISDN line.
E164 End	The ending number in the range of available extensions to assign automatically to IP devices.
Routing/Bandwidth	
Internet calls are not allowed	Disables call routing through the Internet.
Allowed via H.323 aware firewall	<p>Enables call routing through the Internet, using an H.323-aware firewall.</p> <p>Notes</p> <ul style="list-style-type: none"> For an outbound call to the Internet, you must enter the firewall gateway service (e.g. a Polycom VBP appliance) code before the IP address in the dial string. If you select Allowed via H.323 aware firewall you must create a site link between this site and the Internet/VPN site.

Field	Description
Allowed via H.323 aware SBC or ALG	<p>Enables call routing via the Internet, using an H.323-aware SBC (Session Border Control) or ALG (Application Level Gateway) server.</p> <p>Note</p> <p>For an outbound call to the Internet, you must enter the firewall gateway service (for example, a Polycom VBP appliance) code before the IP address in the dial string.</p>
Call Signaling IP Address	IP address of the SBC or ALG server. Supports only IPv4 addresses.
Port	Port address of SBC or ALG server.
Send Unmodified Dial String to SBC/ALG	<p>Select this option if your SBC or ALG requires that the original dial string is passed to it. For example, an H.323 Annex O dial string such as user@company.com is passed directly to the SBC or ALG instead of resolving company.com to an IP address.</p> <p>Deselect this option if your equipment requires a dial string that is converted from company.com to gatekeeper IP address. This option is appropriate for the Polycom VBP.</p>
Total Bandwidth	The total bandwidth of the pipe at the site.
Call Max Bit Rate	The maximum bandwidth that can be used for each intrasite call at the site. The default and maximum value is 2000000 (2 GB).
Subnets	
Subnet IP Address/Mask	<p>Specifies the subnets within the site. For each subnet, includes:</p> <ul style="list-style-type: none"> • IP Address range • Subnet mask • Maximum bandwidth for the subnet • Maximum bit rate per call for the subnet
Enterprise Directory Settings— Endpoint Enterprise Directory security group settings	
Universal Security Group Filter	When in secure mode, search and select groups that are provisioned to the endpoints to represent the valid lists of users that can log in as a user or administrator. If a user is not a member of one of the selected groups then the user is denied access to the endpoint.
Enterprise Directory Admin Group	
Enterprise Directory User Group	

Site Links

The **Site Links** page lists the links defined in the site topology. A link can connect two sites, or it can connect a site to an MPLS network cloud (see [“Network Clouds”](#) on page 102).

Use the commands in the **Actions** list to add, edit, or delete a site link. See [“Add/Edit Site Link Dialog Box”](#) on page 392 for a description of the fields in the site list.

Add/Edit Site Link Dialog Box

Use the **Add Site Link** dialog box to define a new site link in the CMA system’s site topology. Use the **Edit Site Link** dialog box to redefine an existing site link. A site link can connect two sites, or it can connect a site to an MPLS network cloud.

The following table describes the fields in the **Add Site Link** and **Edit Site Link** dialog boxes.

Field	Description
Name	A meaningful name for the site (up to 128 characters).
Description	A brief description of the site (up to 200 characters).
From site	The originating site of the link. The drop-down list includes all defined sites and the Internet. Can’t be changed for a site-to-cloud link.
To site	The destination site of the link. The drop-down list includes all defined sites and an Internet/VPN option. Can’t be changed for a site-to-cloud link.
Total bandwidth (Mbps)	Specifies the total bandwidth limit for this link.
Call Max bit rate (kbps)	Specifies the per-call bandwidth limit for this link.

Site-to-Site Exclusions

The **Site-to-Site Exclusions** page contains a list of the direct site-to-site connections that the system won’t permit a call or session to use.

Use the commands in the **Actions** list to add and delete site-to-site exclusions. The following table describes the fields in the list.

Column	Description
From/To Site	Name of one of the two sites connected by the excluded link.
To/From Site	Name of the other site.

Territories

The **Territories** page contains a list of the territories defined in the site topology. On the right, it displays information about the selected territory.

A territory is a set of one or more sites for which a CMA system is responsible. By default, there is one territory named Default CMA Territory, and its primary node (the CMA system responsible for it) is set to this system.

Use the commands in the **Actions** list to add, edit, or delete a territory. See [“Add/Edit Territory Dialog Box”](#) on page 393 for a description of the fields in the territory list.

Add/Edit Territory Dialog Box

Use the **Add Territory** dialog box to define a new territory in the CMA system's site topology. Use the **Edit Territory** dialog box to define a new territory in the CMA system's site topology.

The following table describes the fields in the **Add Territory** and **Edit Territory** dialog boxes.

Field	Description
Territory Info	
Name	A meaningful name for the territory (up to 128 characters).
Description	A brief description of the territory (up to 200 characters).
Primary Node	The primary node of the CMA system responsible for this territory.
Backup Node	The second node, if any, of the CMA system responsible for this territory.
Associated Sites	
Search Sites	Enter search string or leave blank to find all sites.
Search Result	Lists sites found and shows the territory, if any, to which each currently belongs. Select a site and click the right arrow to move it to the Selected Sites list.
Selected Sites	Lists sites selected and shows the territory, if any, to which each currently belongs.

Network Clouds

The **Network Clouds** page contains a list of the MPLS (Multiprotocol Label Switching) network clouds defined in the site topology.

Use the commands in the **Actions** list to add, edit, or delete an MPLS cloud. See the Cloud Info section of the “[Add/Edit Network Cloud Dialog Box](#)” on page 394 for a description of the fields in the **Network Clouds** list.

Add/Edit Network Cloud Dialog Box

Use the **Add Network Cloud** dialog box to define a new MPLS network cloud in the CMA system’s site topology. Use the **Edit Network Cloud** dialog box to redefine an existing MPLS network cloud.

The following table describes the fields in the **Add Network Cloud** and **Edit Network Cloud** dialog boxes.

Field	Description
Cloud Info	
Name	A meaningful name for the cloud (up to 128 characters).
Description	A brief description of the cloud (up to 200 characters).
Linked Sites	
Search Sites	Enter search string or leave blank to find all sites.
Search Result	Lists sites found and shows the territory, if any, to which each belongs. Select a site and click the right arrow to open the Add Site Link dialog box.
Selected Sites	Lists sites linked to the cloud and shows the territory, if any, to which each belongs.

Polycom CMA System Gatekeeper Functionality

The CMA system gatekeeper provides address translation and network access control services for endpoints, gateways, and MCUs. It also provides other services such as bandwidth management and dial plans services. These additional features allow you to configure and manage your gatekeeping operations and provide flexibility and scalability.



Note

If your system is in maximum security mode, the CMA system gatekeeper functionality is not available.

Default, Redundant, Alternate, and Neighboring Gatekeepers

Default Gatekeeper

Typically during the **First Time Setup** process, the CMA system is designated as the default gatekeeper and the default gatekeeper settings are implemented. The CMA system as the default gatekeeper responsible for:

- Default, alternate and neighboring gatekeeper management
- Device registration
- Address resolution
- Bandwidth control and management
- Call control signaling
- Call management, authorization, access, and accounting
- Firewall traversal

When a call originates from the CMA system and the system is unable to resolve the dialed address, the call can be forwarded to another gatekeeper for resolution. To enable call forwarding, create a neighboring region and a dialing rule that routes calls using a particular prefix to the neighboring gatekeeper.

We recommend keeping the CMA system as the default gatekeeper, so that all endpoints and other devices on the network capable of automatic registration will register with it. This allows the CMA system to serve as the centralized manager of the network and more effectively aid in bandwidth management, firewall traversal, and device authentication and authorization.



Note

MCUs that register with a GRQ instead of a RRQ like the Polycom RMX system, will only register with the CMA system when it is enabled as the default gatekeeper for the zone.

Redundant Gatekeeper

When the CMA system is deployed in a redundant configuration, the redundant CMA system operates as a redundant gatekeeper in parallel with the primary CMA system sharing endpoint registration information. If the primary CMA system becomes unavailable, the redundant CMA system replaces it until it returns.

Alternate Gatekeeper

Within the CMA system, you can designate an alternate gatekeeper. In this case, when an endpoint or other device registers with the CMA system gatekeeper, the system sends back the alternate gatekeeper information to the endpoint. Then, if communication with the CMA system fails, the endpoint will attempt to register with the alternate gatekeeper.

In a redundant configuration, the alternate gatekeeper is the third gatekeeper in line after the primary and redundant CMA system gatekeepers.

Neighboring Gatekeeper

Neighboring gatekeepers are gatekeepers that manage other H.323 regions within an enterprise. When a call originates within one gatekeeper region but that region's gatekeeper is unable to resolve the dialed address, it is forwarded to the neighboring gatekeepers for resolution.



Note

A neighboring gatekeeper may require additional configuration to completely integrate with the CMA system gatekeeper. Also, not all CMA system parameters correspond to parameters on a neighboring gatekeeper.

Within the CMA system, you can also set up a dial rule that will route calls with designated prefixes to designated neighboring gatekeepers.

Device Registration

The CMA system manages device registration and offers several choices from an open registration policy to more restrictive registration policies.

No matter what the gatekeeper registration policy, any endpoint that is automatically provisioned, any endpoint that is registered with the Global Address Book, and any endpoint that is added manually to the CMA system can automatically register with the gatekeeper.

The CMA system gatekeeper registration policies include:

Allow Registration of All Endpoints

This open **Allow Registration of All Endpoints** registration policy allows any device that can find the CMA system gatekeeper to register with it. This is the default policy.

In this case, devices can register to the CMA system automatically:

- When the device broadcasts a message to find a gatekeeper with which to register. In this case, specifying a default gatekeeper is important, because devices that register automatically may find multiple gatekeepers.

Devices register with the system designated as the default gatekeeper, unless that gatekeeper is down. Then devices register with the system designated as the alternate gatekeeper.

When registering, devices send a variety of settings to the gatekeeper including their IP address, one or more H.323 IDs, and one or more E.164 aliases. These settings appear in the CMA system as **Device Details**.

- When devices in dynamic management mode are automatically provisioned by the CMA system.

And devices can be registered to the CMA system manually:

- At the device by specifying the IP address of the CMA system as the gatekeeper.
- At the device by specifying the IP address of the CMA system as the Global Directory Service. Once the device in the CMA system Global Address Book it is registered to the system.
- At the CMA system by adding the device to the one of the device lists (Endpoint, MCU, VBP, or DMA lists).

Once an endpoint is registered, users of other registered endpoints can call the endpoint by using either the H.323 ID, a URI, an E.164 alias, or one of the services.

Allow Registration of Predefined Endpoints Only

The restrictive **Allow Registration of Predefined Endpoints Only** registration policy allows devices to automatically register once they are added to the CMA system either when they are automatically provisioned, automatically registered to the Global Address Book, or added to the system manually.

Allow Registration of Endpoints in Defined Sites

The moderately open **Allow Registration of Endpoints in Defined Sites** registration policy allows endpoints to automatically register if they are within one of the Dial Plan sites defined to the CMA system, when they are automatically provisioned, when they are automatically registered to the Global Address Book, or when they are added to the system manually.

Allow Registration of Predefined Prefixes Only

With this controlled registration policy, devices within a range of defined E.164 prefixes may automatically register with the CMA system.

Routing Mode

The CMA system has two routing modes.

Direct Mode

In this simplest gatekeeper mode, the CMA system gatekeeper resolves IP addresses to their E.164 addresses and aliases (similar to the function of a domain name server) and grants endpoints permission to place calls. Once the gatekeeper performs these two functions, it plays no further role in the call. Call signaling and media streams are sent directly between the endpoints in the call.

In **Direct** mode, the number of concurrent calls supported by a CMA system is derived from the number of device licenses at a 3/5 ratio (calls/devices). So, for example, a system in **Direct** mode licensed for 5000 devices supports up to 3000 calls.

Use **Direct** mode when implementing a hierarchical architecture. A hierarchical architecture is one with multiple gatekeepers, where one gatekeeper—the CMA system in **Direct** mode—acts as the directory gatekeeper at the top of the hierarchy. On the directory gatekeeper, you must configure all of the other member gatekeepers as neighbors and on the member gatekeepers you must configure the directory gatekeeper as a neighbor. However, the member gatekeepers do not have to be neighbored with each other.

When in **Direct** mode, some advanced CMA system features do not work. These features include Simplified Dialing, Conference on Demand, Alternate Routing, Least Cost Routing, MCU board hunting, and firewall traversal for a Polycom VBP system in "Enterprise" or "E" mode. (Firewall traversal for a Polycom VBP system in "Service Provider" or "S" mode does work.)

The advantage of **Direct** mode is that conferences stay connected even if the gatekeeper fails.

The disadvantage of **Direct** mode (along with the loss of advanced functionality) is that during a failure and restart the gatekeeper loses track of active calls that it was not involved in setting up. In this case, after a failure and restart, the gatekeeper's bandwidth calculations will be incorrect until those calls end. Also, since the Conference Monitoring function uses gatekeeper data, the monitoring information for those calls may be incorrect or incomplete.

Routed Mode

In this advanced mode, the CMA system gatekeeper, besides performing the functions of a **Direct** mode gatekeeper, also acts as a proxy for the call signaling H.225 messages that set up the call. In this mode, only the media streams are sent directly between the endpoints in the call.

In **Routed** mode, the number of concurrent calls supported by a CMA system is derived from the number of device licenses at a 3/10 ratio (calls/devices). So, for example, a system in **Routed** mode licensed for 5000 devices supports up to 1500 calls.

The advantage of **Routed** mode is that it enables advanced features such as Simplified Dialing, Conference on Demand, Alternate Routing, Least Cost Routing, MCU board hunting and firewall traversal for a Polycom VBP system in "Enterprise" or "E" mode. Routed mode is also supported for the Polycom VBP system in "Service Provider" or "S" mode.

The disadvantage of routed mode is that a gatekeeper failure and restart terminates all running conferences that include a registered device. Calls are not reestablished after a system failure and restart. Conferences show a status of **Active**, but participants show a status of **Disconnected**.

In either mode, CDR information for calls is accurate if the CMA system does not fail and the endpoints send a DRQ (Disconnect Request) at the end of the call.

Polycom CMA System Integration with Microsoft Outlook

Polycom now supports two conferencing methods when integrating Polycom conferencing with Microsoft Outlook: Reserved and Reservationless.



Note

If you wish to implement both reserved conferencing (enabled by a CMA system) and reservationless or ad hoc conferencing (enabled by a Polycom DMA system), you should create two pools of RMX bridges as described in "[DMA View](#)" on page 225. However if you do, Polycom does not recommend using both the Polycom Scheduling Plug-in for Microsoft Outlook (Reserved Conferencing) and the Polycom Conferencing Add-in for Microsoft Outlook (Reservationless Conferencing) on the same client system.

Standard Polycom CMA System and Reserved Conferencing

Reserved conferencing is standard with the CMA system. All conferences scheduled either through the CMA system web scheduler or one of the Scheduling Plugins are reserved conferences, which means the CMA system reserves video bridge, network resources, and video endpoints at the scheduled time. In this case, the calendars for the endpoints are stored and maintained by the CMA system.

When the conference is scheduled using the Scheduling Plugin for Microsoft Outlook and the participants use Microsoft Outlook as their E-mail and calendaring tool, the scheduled conferences are also posted as meetings on the participants' Outlook calendars. However, the endpoints themselves do not have Outlook calendars.

Polycom Conferencing for Microsoft Outlook, Reservationless Conferencing, and Calendaring Management

The CMA system can also be used to provision Polycom Conferencing for Microsoft Outlook, which is reservationless conferencing. When you use this method:

- Video bridge, network resources, and video endpoints are not reserved at the scheduled time.
- A Polycom RMX or DMA system is required to locate available bridge resources when the meeting begins.
- Calendars for the endpoints are stored and maintained by Microsoft Exchange and the endpoints have their own Outlook calendar.

Polycom Conferencing for Outlook, which requires the Polycom Conferencing Add-in, allows:

- Conference organizers to:
 - Use Microsoft Outlook and its usual meeting request workflow to schedule video- and audio-enabled meetings.
 - Include recording and streaming into the conference, when required.
- Meeting participants to:
 - Track their video- and audio-enabled meetings on the same calendar that they track their other meetings.
 - Click a link in an E-mail meeting request to join conferences on their associated video or audio endpoint system.
- Endpoints to have their own unique credentials and mailbox separate from the endpoint user, so that endpoints can display their own calendars. This is especially important for room endpoints.

The CMA system supports the Polycom Conferencing for Outlook solution. It allows you to provision endpoints with the credentials, mailbox address, Exchange server IP address, and calendaring service settings they need to use Polycom Conferencing for Outlook.

To provision endpoints with the information required to support Polycom Conferencing for Outlook, you must complete the following tasks (after your sites are set up):

- 1 [“Associate Sites with Microsoft Exchange Servers”](#) on page 405.
- 2 [“Assign Calendaring Settings to Provisioning Profiles”](#) on page 406.
- 3 [“Provision the Exchange Mailbox for Calendaring Service-enabled Endpoints”](#) on page 407.

Polycom CMA System Integration with Microsoft Lync Server 2010 or Microsoft Office Communications Server 2007

The CMA system supports the integration of selected Polycom endpoints with Microsoft® Lync™ Server 2010 or Microsoft® Office Communications Server 2007. Integration with these unified communications servers allows Polycom HDX system users to see client users who have been added to the Polycom HDX system **Favorites** list and place audio and video calls to them. Conversely, client users can also see Polycom HDX system users in their client Contacts List and place audio and video calls to them.

For Polycom HDX systems that are integrated with a Lync or Office Communications server, the unified communications server replaces the CMA system as the presence and directory service provider. However, the CMA system continues to act as the gatekeeper and manager for these endpoint systems.

The CMA system supports the integration with these unified communications servers by provisioning endpoints with the credentials, Exchange server IP address, and communications service settings they need.

To provision endpoints with the information required to integrate with these unified communications servers, you must complete the following tasks:

- 1 [“Integrate with Microsoft Lync Server 2010 or Microsoft Office Communications Server 2007”](#) on page 407.
- 2 [“Provision SIP Settings for Microsoft Lync or Microsoft Office Communications Server Integration”](#) on page 408.

Endpoint Directory and Directory Settings

When an endpoint registers with the CMA system, its information is automatically entered into the Global Address Book. When information changes at the endpoint, the Global Address Book is automatically updated as well. If an endpoint is configured to **Allow Directory Changes**, additions and deletions to the Global Address Book are pushed to the endpoint.

Endpoints that get their global directory from the CMA system will either get the Global Address Book or the enterprise LDAP directory. Two **Directory Setup** options allow you to affect which devices and users appear in the endpoint directory.

Typically, standard endpoints (those that are not dynamically managed) register for the Polycom GDS and are listed in the CMA system Global Address Book. The Global Address Book allows standard endpoint users to call other standard endpoint users by selecting them by name. In this case, the Global Address Book is limited to 2000 entries, which is the limit that standard endpoint systems can manage.



Notes

- The CMA system Global Address Book lists endpoints. Endpoints may or may not have users or rooms associated with them. On an endpoint, the Global Address Book does not list users unless they have endpoints associated with them.
- If your company has more than 100 endpoints, don't limit the Global Address Book on the endpoint side or the endpoint user won't have access to all Global Address Book entries.
- The CMA system Global Address Book does not support unicode data.

The **Include dynamically-managed devices in the Global Address Book** option changes the Global Address Book so that it includes all standard endpoints and all dynamically-managed endpoints such as CMA Desktop and Polycom VVX 1500 endpoints in the Global Address Book. In this case, the Global Address Book limit is increased to 5000 entries. (Dynamically-managed endpoints are always included in the enterprise LDAP directory.)

By default the **Include dynamically-managed devices in the Global Address Book** option is selected. This brings all of your devices and users together into one endpoint directory. However, you may not want to take advantage of this feature if you have legacy endpoint systems such as VSX, ViewStation, and FX endpoints. These endpoint systems cannot handle the increased size of the Global Address Book. For information on clearing this option, see [“Remove or Include Dynamically-Managed Endpoints in the Global Address Book”](#) on page 368.

The second **Directory Setup** option affects both the Global Address Book and the enterprise LDAP directory. The CMA system Guest Book includes static user entries. By selecting the **Show Guest Book entries in the Directory**, these static entries are included in the endpoint directory, regardless of whether the endpoint directory is the Global Address Book or the enterprise LDAP directory. The **Show Guest Book entries in the Directory** option is also selected by default.

Server Setting Operations

This chapter describes how to update the Polycom® Converged Management Application™ (CMA®) system configuration settings, many of which were entered during **First Time Setup**. It includes these topics:

- [Edit the Polycom CMA System Network Settings](#)
- [Edit the Polycom CMA System Time Settings](#)
- [Integrate with Microsoft Exchange Server for Calendaring Management](#)
- [Integrate with Microsoft Lync Server 2010 or Microsoft Office Communications Server 2007](#)
- [View Current Polycom CMA System Licensing](#)
- [Add Polycom CMA System Licenses](#)
- [Reclaim Polycom CMA Desktop Licenses](#)
- [Add or Remove a Polycom CMA System Custom Logo](#)
- [Add or Remove a Polycom CMA System Custom Logo](#)
- [Add or Remove a Polycom CMA Desktop Custom Logo](#)

Edit the Polycom CMA System Network Settings

Edit the system **Network** settings to change the basic network information for the CMA system.



Note

Changing the IP address via the **Windows Network Settings** is not a supported operation. To change the CMA system IP address, you must use this procedure.

To edit the CMA system network settings

- 1 Go to **Admin > Server Settings > Network**.

- 2 Configure these settings on the **Network** page, as necessary.

Field	Description
System Name	The NetBIOS name (ASCII only) of the CMA system server. Must be between 6 and 16 characters long; dashes and underscores are valid characters.
IPv4 Address	The static IPv4 address for the CMA system.
IPv4 Subnet Mask	The network subnet mask for the CMA system IP address.
IPv4 Default Gateway	The static IP address of the CMA system gateway.
DNS Domain	<p>The DNS domain name suffix for the network in which the domain name server and CMA system server reside. For example <code>polycom.com</code>, not the fully qualified path of <code><hostname>.polycom.com</code>.</p> <p>Note</p> <p>If instead of entering a single domain controller, you enter an FQDN that maps to multiple servers, be sure that all of the mapped servers are directory domain controllers with global catalogs.</p>
Preferred DNS Server	The IP address of the preferred domain name server for the network.
Alternate DNS Server	The IP address of the alternate domain name server for the network.

- 3 Click **Update**.

If you change the IP address, the system prompts you to restart the CMA system. We also recommend that you restart the system if you change the subnet mask.

- 4 As required, restart the system.

Edit the Polycom CMA System Time Settings

Edit the **System Time** server settings to change the CMA system server time or to synchronize the server with an external NTP server.

To edit the CMA system time settings

- 1 Go to **Admin > Server Settings > System Time**.

- 2 Configure these settings on the **System Time** page, as necessary.

Field	Description
System Time Zone	The time zone in which the CMA system server resides.
Auto adjust for Daylight Saving?	Select this option to adjust the clock automatically for daylight savings time.
Use Current Time	Select this option to input the current date and time.
Use External NTP Server Time Synchronization	Select this option to synchronize the CMA system date and time with an external NTP server.
IP address or DNS resolved name	The IP address or fully qualified domain name (ASCII only) of the NTP server. If needed, enter multiple servers separated by a space.



Note

Make sure the current system time is correct before synchronizing with an NTP server. If you set the system to use an external NTP server when the current date and time are incorrect, the system time may be wrong for the amount of time specified in the **Minutes between synchronization attempts**.

- 3 Click **Update**.

Integrate with Microsoft Exchange Server for Calendaring Management

The CMA system supports the Polycom Conferencing for Outlook solution. It allows you to provision endpoints with the credentials, mailbox address, Exchange server IP address, and calendaring service settings they need to use Polycom Conferencing for Outlook.

This section describes the tasks that enable provisioning endpoints for Polycom Conferencing for Outlook.

Associate Sites with Microsoft Exchange Servers

By default, the CMA system is set up to automatically discover the Exchange server for the domain in which a site is located. However, if you wish to associate sites with an Exchange server using its IP address or DNS name, follow this procedure.

To associate sites with Microsoft Exchange servers by IP address or DNS name

- 1** Go to **Admin > Server Settings > Calendaring Management**.
- 2** In the **Manage Calendaring** dialog box, click **Calendared Sites**.
The **Specify Calendaring Exchange Servers** page appears listing the sites defined on the CMA system.
- 3** Select the check box for each of the sites you need to associate with a single Exchange server and then click **Specify Exchange Server**.
- 4** In the **Add Exchange Server** dialog box, enter the **Exchange Server Address** or DNS and click **Save**.
The sites appear in the calendared sites list below.
- 5** Repeat steps **3** and **4** for each Exchange server for which you need to associate sites.

Assign Calendaring Settings to Provisioning Profiles

Calendaring settings are included as part of provisioning profiles.

To assign calendaring settings to provisioning profiles

- 1** Go to **Admin > Server Settings > Calendaring Management**.
- 2** In the **Manage Calendaring** dialog box, click **Group Information**.
The **Group Information** page appears listing the provisioning profiles defined on the CMA system.
- 3** Select the check box for each of the provisioning profiles to which you need to assign the same calendaring settings and then click **Specify Options**.
- 4** In the **Manage Calendaring** dialog box, configure these options.

Fields	Description
Meeting Reminder Time	Specifies the number of minutes before the meeting an endpoint system provisioned for Polycom Conferencing for Outlook will display a reminder.
Enable Alert Tone	When enabled, specifies that an endpoint system provisioned for Polycom Conferencing for Outlook will play a sound along with the meeting reminder. In this case, the endpoint will only play a sound when the system is not in a call.
Display Private Meetings	When enabled, specifies that an endpoint system provisioned for Polycom Conferencing for Outlook will display details about meetings marked private.

5 Click Save.

The profiles appear in the calendared profiles list below.

6 Repeat steps 3 through 5 for each set of profiles to which you need to assign calendaring settings.

Provision the Exchange Mailbox for Calendaring Service-enabled Endpoints

To use Polycom Conferencing for Outlook (PCO), a Polycom endpoint system must have a mailbox on the assigned Exchange server, and the Exchange server must authenticate the endpoint before it can access its mailbox.

To use the CMA system to automatically provision a Polycom endpoint system, the endpoint system must use the same credentials (username and password) to access both the Exchange server and the CMA system. Only then can the CMA system automatically provision a calendaring service-enabled endpoint system.

To provision the Exchange Mailbox for calendaring service-enabled endpoints

- 1 Go to Admin > Server Settings > Calendaring Management.**
- 2 In the Manage Calendaring dialog box, click Mailbox.**
- 3 In the Polycom Conferencing for Outlook page, enable Provision Mailbox and click OK.**

For Exchange credentials, each endpoint system will be provisioned with the same credentials it used to access the CMA system.

For its mailbox, each endpoint system will be provisioned with the mailbox configured for it in Active Directory. This mailbox must be pre-configured for the endpoint system on the Exchange server.

Integrate with Microsoft Lync Server 2010 or Microsoft Office Communications Server 2007

The CMA system supports the integration with Microsoft® Lync™ Server 2010 or Microsoft® Office Communications Server 2007 by provisioning endpoints with the group and SIP settings they need.

After you set up integration with Microsoft Lync Server or Office Communications Server, all endpoints receive directory information from one of those servers. You are no longer using the enterprise directory or the other directory functions in the CMA system.

This section describes the tasks that enable provisioning endpoints for integration with Microsoft Lync Server or Office Communications Server.

Provision Group for Microsoft Lync or Microsoft Office Communications Server Integration

You have set up the Microsoft Lync or Office Communications Server group that needs to be provisioned to endpoints in each automatic provisioning profile. This controls the directory that endpoints can see.



Notes

- You cannot provision integration with a Microsoft Lync or Office Communications Server via scheduled provisioning.
- If the endpoint being provisioned is not capable of integration with a Microsoft Lync or Office Communications Server, the endpoint will ignore this settings.
- The group setting here applies to both Microsoft Lync and Office Communication Server.

To provision integration with Microsoft Lync or Office Communications Server

- 1 Go to **Admin > Provisioning Profiles > Automatic Provisioning Profiles**.
- 2 In the **Automatic Provisioning Profiles** page, select the profile of interest and click **Edit**.
- 3 In the **Provisioning Fields** dialog box, click **Microsoft Lync Settings** and enter a **Group Name**.

The Group Name is the group set in the Microsoft Lync Server or Office Communication Server.
- 4 Click **OK**.

Provision SIP Settings for Microsoft Lync or Microsoft Office Communications Server Integration

By default, SIP is disabled in site provisioning. This procedure describes how to change existing site provisioning settings so that they provision integration with one of these unified communications servers.

To integrate with a Microsoft Lync or Office Communications Server, Polycom endpoints must have a user account on the Microsoft unified communications server infrastructure. To have the CMA system automatically provision a Polycom endpoint for this integration, the endpoint must use the same credentials (username and password) to access both the unified communications server and the CMA system. Only then can the CMA system automatically provision a calendaring service-enabled endpoint system.

To provision SIP for integration with Microsoft Lync or Office Communications Server

- 1 Go to **Admin > Dial Plan and Sites > Sites**.
- 2 In the **Sites** page, select the site of interest and click **Edit Site Provisioning Details**.
- 3 In the **Edit Site Provisioning Details** dialog box, click **SIP Settings** and select these options.

Settings not listed below are optional, based on the configuration of your systems

Fields	Description
Enable SIP	Specify whether to enable SIP calls.
Automatically Discover SIP Servers	The CMA system will issue a DNS query to locate the SIP server and provision that information to endpoints.
Proxy Server	Specify the IP address or DNS name of the SIP proxy server for the network.
Registrar Server	Specify the IP address or DNS name of the SIP registrar server for the network. <ul style="list-style-type: none"> In an Microsoft Office Communications Server 2007 or Microsoft Lync Server 2010 environment, specify the IP address or DNS name of the Office Communications Server or Lync Server server. If registering a remote HDX system with an Office Communications Server Edge Server or Lync Server Edge Server, use the fully qualified domain name of the access edge server role.
Backup Registrar Server	Specify the IP address or DNS name of a backup SIP registrar server for the network
Transport Protocol	Indicates the protocol the system uses for SIP signaling. The SIP network infrastructure determines which protocol is required. <ul style="list-style-type: none"> Auto enables an automatic negotiation of protocols in the following order: TLS, TCP, UDP. This is the recommended setting for most environments. TCP provides reliable transport via TCP for SIP signaling. UDP provides best-effort transport via UDP for SIP signaling. TLS provides secure communication of the SIP signaling. TLS is available only when the system is registered with a SIP server that supports TLS. When you choose this setting, the system ignores TCP/UDP port 5060..

Fields	Description
SIP Server Type	Specify whether the SIP registrar server is a Microsoft Office Communications Server or a Microsoft® Lync™ Server 2010. Enabling this setting activates integration features such as the Microsoft global directory and Office Communicator contact sharing with presence.
Verify Certificate	Enable this option when the endpoint system's certificate should be verified by the certificate authority.
Use Enterprise Credentials	Enable this option when the endpoint system should use the credentials the user entered at the endpoint to use for authentication when registering with a SIP registrar server.
User Name	Specify the name to use for authentication when registering with a SIP registrar server, for example, <i>msmith@company.com</i> . If the SIP proxy requires authentication, this field and the password cannot be blank.
Password	Specify the password that authenticates the system to the registrar server.

- 4 Click OK.

View Current Polycom CMA System Licensing

To view current CMA system licensing

- Go to **Admin > Server Settings > Licenses**.

The **Active License** section of the **Licenses** page displays the following information.

Field	Description
Activation Key	The current activation key for the product.
Expiration Date	The expiration date of the current license key.
Components	The components for which the CMA system is licensed.
Seats	The number of seats for which the CMA system is licensed.

Add Polycom CMA System Licenses

Adding licenses to your CMA system is a two step process:

- [Request a Software Activation Key Code.](#)
- [Enter the Polycom CMA System Activation Key](#)

These processes are described in the following topics.

Request a Software Activation Key Code

To request a software activation key code

- 1 In a separate browser page or tab, log into the CMA system server as an administrator.
- 2 Go to **Admin > Server Settings > Licenses** and record the CMA system server serial number:
_____.
- 3 Go to <http://support.polycom.com>.
- 4 In the **Licensing & Product Registration** section, select **Activation/Upgrade**.
- 5 Log in or **Register for an Account**.
- 6 Select **Site & Single Activation/Upgrade**.
- 7 In the **Site & Single Activation** page, enter the serial number you recorded in step 2.
- 8 Click **Next**.
- 9 Accept the **EXPORT RESTRICTION** agreement.
- 10 In the new **Site & Single Activation** page, enter the software license number listed on your License Certificate (shipped with the product) and click **Activate**.
- 11 When the activation key appears, record it:
_____ - _____ - _____ - _____
- 12 Repeat this procedure for each additional license key required.

Enter the Polycom CMA System Activation Key

To enter the CMA system activation key

- 1 Go to **Admin > Server Settings > Licenses**.

- 2 Enter the new activation key into the **Add New License > Activation Key** field and click **Add**. (Note that the field is ASCII only.)

Reclaim Polycom CMA Desktop Licenses

To set the threshold for reclaiming inactive Polycom CMA Desktop licenses

- 1 Go to **Admin > Server Settings > Licenses**.
- 2 Change the **Threshold** value in the **Reclaim Inactive CMA Desktop Licenses** section of the **Licenses** page. To reclaim licenses more quickly, lower the threshold. Set the threshold to zero, to stop reclaiming licenses.
- 3 Click **Update**.

Add or Remove a Polycom CMA System Custom Logo

You can add your company's logo to the CMA system user interface. To avoid distortion, we recommend adding a logo in GIF, JPG, or PNG format with a size of 300 x 44 pixels.

To add a custom logo to the CMA system user interface

- 1 Go to **Admin > Server Settings > Custom Logos**.
- 2 In the **Current Logo** section of the **Custom Logos** page, click **Upload...**
- 3 In the **Select file** dialog box, browse to the logo image and select the file.
- 4 Click **Open**.
- 5 In a redundant configuration, repeat steps 1 through 4 on the redundant server.

To remove a custom logo from the CMA system user interface

- 1 Go to **Admin > Server Settings > Custom Logos**.
- 2 In the **Current Server Logo** section of the **Custom Logos** page, click **Remove**.

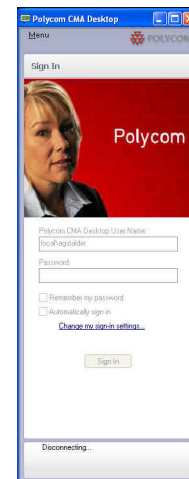
Add or Remove a Polycom CMA Desktop Custom Logo

You can add your company logo to the Polycom CMA Desktop user interface. This logo will be displayed on the application user interface before the user logs in. The following illustration shows the default Polycom CMA Desktop user interface and a customized Polycom CMA Desktop user interface.

Default Polycom CMA Desktop



Branded Polycom CMA Desktop



To avoid distortion, use a logo in GIF or JPG format with a size of approximately 260x215 pixels.

Because the Polycom CMA Desktop logo is stored in the CMA system database, in redundant configurations you do not need to upload the logo to both servers.

To add a custom logo to the CMA Desktop user interface

- 1 Go to **Admin > Server Settings > Custom Logos**.
- 2 In the **Current CMA Desktop Logo** section of the **Custom Logos** page, click **Upload...**
- 3 In the **Select file** dialog box, browse to the logo image and select the file.
- 4 Click **Open**.

Once a user logs in, is provisioned, and then logs out, the logo will be displayed on the Polycom CMA Desktop user interface.

To remove a custom logo from the CMA Desktop user interface

- 1 Go to **Admin > Server Settings > Custom Logos**.

- 2 In the **Current CMA Desktop Logo** section of the **Custom Logos** page, click **Restore Default**.

Once a user logs in, is provisioned, and then logs out, the default logo will be displayed on the CMA Desktop user interface.

Edit the Polycom CMA System E-mail Account

To edit the CMA system e-mail account

- 1 Go to **Admin > Server Settings > E-mail**.
- 2 On the **E-mail** page, edit the e-mail account (ASCII only) from which the CMA system will send conference notification e-mails or edit the IP address of the mail server from which the CMA system will send conference notification e-mails.



Notes

- Many e-mail servers will block or discard e-mails without a qualified From: address. To avoid this issue, make sure each person with Scheduler permissions has a valid E-mail address.
- Many E-mail servers will block or discard E-mails from un-trusted domains, in which case you may need to change the default CMA system E-mail address to one in a trusted domain.

- 3 Click **Update**.

Polycom CMA System SNMP

This chapter provides a discussion of the Polycom® Converged Management Application™ (CMA®) SNMP support. It includes these topics:

- [SNMP Overview](#)
- [Polycom CMA System SNMP Operations](#)
 - [Enable SNMP Messaging](#)
 - [Edit the SNMP Settings for a Polycom CMA System](#)
 - [Add an SNMP Notification Receiver](#)
 - [Configure Alert Thresholds](#)
 - [Download Polycom CMA System MIB Package](#)
 - [Change the SNMP Communication Port](#)

SNMP Overview

Simple Network Management Protocol (SNMP) is a TCP/IP-based communication protocol that allows network management systems to manage resources across a network.

SNMP communication takes place between the management system and SNMP agents, which are the hardware and software that the management system monitors. An agent collects and stores local system information and makes this information available to the management system via SNMP.

The CMA system software includes an SNMP agent. It translates local system information into the format defined by the MIB.

The CMA system resides on a Polycom-branded Dell server. The Dell server software also includes an SNMP agent and MIB. However, the CMA system acts as a proxy agent to forward the Dell server MIB alarms and alerts, so the management system does not need to be configured to receive information directly from the Dell server MIB.

Polycom recommends using a MIB browser to explore the CMA system MIB. A copy of the MIB can be downloaded from the CMA system. For more information go to [“Download Polycom CMA System MIB Package”](#) on page 422. The CMA system MIB is self-documenting including information about the purpose of specific traps and inform notifications.

It is important to note that you should understand how your SNMP management system is configured to properly configure the CMA system SNMP transport protocol requirements, SNMP version requirements, SNMP authentication requirements, and SNMP privacy requirements on the CMA system.

The CMA system supports three SNMP levels:

- **Disabled** – The CMA system SNMP processes are turned off.
- **SNMPv2c** – The CMA system implements a sub-version of SNMPv2. The key advantage of SNMPv2c is the Inform command. Unlike Traps, Inform messages are sent to the management system that must be positively acknowledged with a response message. If the management system does not reply to an Inform, the CMA system resends the Inform. SNMPv2c also has improved error handling and improved SET commands.

One drawback of SNMPv2c is that it is subject to packet sniffing of the clear text community string from the network traffic, because it does not encrypt communications between the management system and SNMP agents.

- **SNMPv3** – The CMA system implements the newest version of SNMP. Its primary feature is enhanced security. The *contextEngineID* in SNMPv3 uniquely identifies each SNMP entity. The *contextEngineID* is used to generate the key for authenticated messages.

The CMA system implements SNMPv3 communication with authentication and privacy (the *authPriv* security level as defined in the USM MIB).

- Authentication is used to ensure that traps are read by only the intended recipient. As messages are created, they are given a special key that is based on the *contextEngineID* of the entity. The key is shared with the intended recipient and used to receive the message.
- Privacy encrypts the SNMP message to ensure that it cannot be read by unauthorized users.

Polycom CMA System SNMP Operations

This section describes the CMA system SNMP operations including:

- [Enable SNMP Messaging](#)
- [Edit the SNMP Settings for a Polycom CMA System](#)
- [Add an SNMP Notification Receiver](#)
- [Configure Alert Thresholds](#)
- [Download Polycom CMA System MIB Package](#)

Enable SNMP Messaging

To enable SNMP messaging you must perform the two tasks:

- [Edit the SNMP Settings for a Polycom CMA System](#)
- [Add an SNMP Notification Receiver](#)

Edit the SNMP Settings for a Polycom CMA System

To edit the SNMP settings for a CMA system

- 1 Go to **Admin > SNMP Settings**.
- 2 To enable SNMP, select an **SNMP Version**. For information on the SNMP versions, see [“SNMP Overview”](#) on page 415.
- 3 Configure these settings for the connection between the CMA system and the SNMP agents on the **SNMP Setting** page.

Setting	Description
Transport	<p>Specifies the transport protocol for SNMP communications. SNMP can be implemented over two transport protocol:</p> <p>TCP—This protocol has error-recovery services, message delivery is assured, and messages are delivered in the order they were sent. Some SNMP managers only support SNMP over TCP.</p> <p>UDP—This protocol does not provide error-recovery services, message delivery is not assured, and messages are not necessarily delivered in the order they were sent.</p> <p>Because UDP doesn't have error recovery services, it requires fewer network resources. It is well suited for repetitive, low-priority functions like alarm monitoring.</p>

Setting	Description
Port	Specifies the port that the CMA system uses for general SNMP messages. By default, the CMA system uses port 161.
Community	<p>For SNMPv2c, specifies the context for the information, which is the SNMP group to which the devices and management stations running SNMP belong.</p> <p>The CMA system has only one valid context—by default, <i>public</i>—which is identified by this Community name. The CMA system will not respond to requests from management systems that do not belong to its community.</p>
V3 Context Name	For SNMPv3, specifies the context for the information. The CMA system has only one valid context, which is identified by <i>contextName</i> (in our case—an empty string) and <i>contextEngineID</i> .
V3 Local Engine Id	For SNMPv3, displays the CMA system <i>contextEngineID</i> for SNMPv3.
Security User	For SNMPv3, specifies the security name required to access a monitored MIB object.
Auth Type	<p>For SNMPv3, specifies the authentication protocol. These protocols are used to create unique fixed-sized message digests of a variable length message.</p> <p>The CMA system implements communication with authentication and privacy (the <i>authPriv</i> security level as defined in the USM MIB).</p> <p>Possible values for authentication protocol are:</p> <ul style="list-style-type: none"> • MD5—Creates a digest of 128 bits (16 bytes). • SHA—Creates a digest of 160 bits (20 bytes). <p>Both methods include the authentication key with the SNMPv3 packet and then generate a digest of the entire SNMPv3 packet.</p>
Auth Password	For SNMPv3, specifies the authentication password that is appended to the authentication key before it is computed into the MD5 or SHA message digest.

Setting	Description
Encryption Type	<p>For SNMPv3, specifies the privacy protocol for the connection between the CMA system and the SNMP agent.</p> <p>The CMA system implements communication with authentication and privacy (the <i>authPriv</i> security level as defined in the USM MIB).</p> <p>Possible values for privacy protocol are:</p> <ul style="list-style-type: none"> • DES—Uses a 56 bit key with a 56 bit salt to encrypt the SNMPv3 packet. • AES—Uses a 128 bit key with a 128 bit salt to encrypt the SNMPv3 packet.
Encryption Password	For SNMPv3, specifies the password to be associated with the privacy protocol.

- 4 Click **Save SNMP Settings**.

Add an SNMP Notification Receiver

You can configure the CMA system to send SNMP messages to different notification receivers (e.g., a network management system).

To add an SNMP notification receiver to a CMA system

- 1 Go to **Admin > SNMP Settings**.
- 2 In the **Notification RCVR Actions** section, click **Add**.
- 3 Configure these settings in the **New Notification Receiver** dialog box.

Setting	Description
IP Address	Specifies the IP address of the host receiver.
Transport	<p>Specifies the transport protocol for SNMP communications to the host receiver. Possible values are:</p> <ul style="list-style-type: none"> • TCP • UDP <p>Select the transport protocol for which the host receiver is configured.</p>
Port	Specifies the port that the CMA system will use to send notifications. By default, the CMA system uses port 162.

Setting	Description
Trap/Inform	<p>Specifies the type of information that should be sent to the host receiver. Possible values are:</p> <ul style="list-style-type: none"> • Inform—An unsolicited message sent to a notification receiver that expects/requires a confirmation message. Introduced with SNMP version 2c, this option is not supported by systems that only support SNMP version 1. • Trap—An unsolicited message sent to a notification receiver that does not expect/require a confirmation message.
SNMP Version	<p>For SNMPv3, specifies the context for the information.</p> <p>The CMA system is a proxy-forwarding application. It passes SNMP requests to its various SNMP-reporting processes based on the context information in the SNMP message. For SNMPv3, this context is identified by <i>contextName</i> and <i>contextEngineID</i>.</p>
V3 Local Engine Id	For SNMPv3, displays the CMA system <i>contextEngineID</i> for SNMPv3.
Security User	For SNMPv3, specifies the security name required to access a monitored MIB object.
Auth Type	<p>For SNMPv3, specifies the authentication protocol. The CMA system implements communication with authentication and privacy (the <i>authPriv</i> security level as defined in the USM MIB).</p> <p>Possible values for authentication protocol are:</p> <ul style="list-style-type: none"> • MD5 • SHA <p>These protocols are used to create unique fixed-sized message digests of a variable length message. MD5 creates a digest of 128 bits (16 bytes) and SHA creates a digest of 160 bits (20 bytes).</p>
Auth Password	For SNMPv3, specifies the authentication password that is appended to the authentication key before it is computed into the MD5 or SHA message digest.

Setting	Description
Encryption Type	<p>For SNMPv3, specifies the privacy protocol for the connection between the CMA system and the notification receiver.</p> <p>The CMA system implements communication with authentication and privacy (the <i>authPriv</i> security level as defined in the USM MIB).</p> <p>Possible values for privacy protocol are:</p> <ul style="list-style-type: none"> • DES • AES
Encryption Password	For SNMPv3, specifies the password to be associated with the privacy protocol.

Configure Alert Thresholds

The CMA system provides administrators with the ability to configure some alert thresholds settings.

To configure alert thresholds

- 1 Go to **Admin > Alert Settings > CMA Alert Threshold Settings**.
- 2 Configure these thresholds:

Threshold	Description
Used disk space alert threshold	<p>Whenever the system disk space usage in a partition (as identified in the CMA Info Dashboard pane) exceeds this threshold, the system sends an alert and an SNMP trap.</p> <p>Valid values for this threshold are between 1-100%. By default, this threshold is set to 90%.</p> <p>A threshold setting of 75% or greater is recommended and no greater than 95%.</p>
Memory usage alert threshold	<p>Whenever the system memory usage (as identified in the CMA Info Dashboard pane) exceeds this threshold, the system send an alert and an SNMP trap.</p> <p>Valid values for this threshold are between 1-100%. By default, this thresh-%old is set to 95%.</p> <p>A threshold setting between 80-95% is recommended.</p>

Threshold	Description
Average CPU usage alert threshold	<p>Whenever the average system CPU usage (over all CPUs as identified in the CMA Info Dashboard pane) exceeds this threshold for the length of time identified in the Average CPU usage alert threshold window, the system sends an alert and an SNMP trap.</p> <p>Valid values for this threshold are between 1-100%. By default, this threshold is set to 95%. A threshold setting between 90-100% is recommended.</p>
Average CPU usage alert threshold window	<p>Whenever the average system CPU usage (over all CPUs as identified in the CMA Info Dashboard pane) exceeds this threshold for the length of time identified in the Average CPU usage alert threshold window, the system sends an alert and an SNMP trap.</p> <p>By default, this threshold window is set to 10 minutes. This threshold can be set to between 1-15 minutes.</p> <p>A threshold setting between 5-10 minutes is recommended.</p>

3 Click **Update**.

Download Polycom CMA System MIB Package

The CMA system enterprise MIB relates information about the system. The information is divided into these categories:

- **Configuration**— The static state of each component, for example component type, software version, current owner, values of all configured parameters.
- **Status**— The dynamic state of each component, for example the number of connections, number of conferences, number of ports (used and available), temperature, fan speed, CPU utilization, memory utilization, network link status, number of dropped packets, jitter measurements, number of successful calls, number of CPU resets.
- **Alerts**— To notify that an exception condition has occurred, for example a power supply failure, link/down up on a major interface, memory usage exceeding a predefined percentage, connections in an MCU exceeding a threshold, a logical fault or ungraceful transition.
- **Conformance**— The historical trend for selected groups of data, for example conference load over time for an MCU, bandwidth consumed over time for a network device.

To download the MIB package for a CMA system

- 1** Go to **Admin > SNMP Settings**.
- 2** Click **Download CMA MIBs**.
- 3** In the **CMA MIBs** dialog box, select the MIB of interest.

Name	Description
Brcm-adapterInfo-MIB	The interface table (ifTable) shows addresses, physical addresses, names, descriptions etc. of the network interfaces
DCS3FRU-MIB	Contains all the field replaceable unit names, serial numbers, and revisions for the Polycom-branded Dell server. For more information, see the Dell SNMP documentation.
DELL-ASF-MIB	Trap definitions for the Polycom-branded Dell server. For more information, see the Dell SNMP documentation.
INET-ADDRESS-MIB	A definition file for standard conventions included for reference.
ITU-ALARM-TC-MIB	A definition file for standard conventions included for reference.
MIB-Dell-10892	The primary MIB for the Polycom-branded Dell server. It provides 36 traps from the server motherboard, including system type, voltages, and temperature readings. For more information, see the Dell SNMP documentation.
MIB-Dell-10900	Trap definitions for the system including up/down, CPU, Memory, Network, and Disk monitoring. For more information, see the Dell SNMP documentation.
MIB-Dell-CM	Provides information about devices running on the Polycom-branded Dell server. For more information, see the Dell SNMP documentation.
POLYCOM-CMA-MIB	CMA-specific MIB definition
RFC1213-MIB	RFC1213MIB definitions included for reference. The CMA system supports all but "egp".
SNMPv2-CONF	A definition file for standard conventions included for reference.

Name	Description
SNMPv2-SMI	A definition file for standard conventions included for reference.
SNMPv2-TC	A definition file for standard conventions included for reference.
StorageManagement-MIB	Monitoring and information about the hard disks and RAID configuration on the server.

Polycom recommends using a MIB browser to explore the CMA system MIB. However, a printed copy of the MIB is available in [“Polycom CMA System SNMP”](#) on page 415. The CMA system MIB is self-documenting including information about the purpose of specific traps and inform notifications.

Change the SNMP Communication Port

By default, the CMA system uses port 161 as its standard open port for SNMP communications. However, you can change this to another open port.

To change the SNMP communication port

- 1 Go to **Admin > SNMP Settings**.
- 2 In the **Port** field of the **SNMP Settings** page, type a new communication port number and click **Update SNMP Settings**.

Database Operations

This chapter describes the Polycom® Converged Management Application™ (CMA®) database integration and operations. It includes these topics:

- [Overview of the Polycom CMA System Database](#)
 - [The following values are recommended for SQL server HD size:](#)
 - [External Databases](#)
 - [Database Restoration](#)
- [Database Operations](#)
 - [Integrate a Polycom CMA System to an External Database](#)
 - [Revert a Polycom CMA System to its Internal Database](#)

Overview of the Polycom CMA System Database

CMA system information is stored in these internal databases:

Database	Description
ReadiManager.bak	The general CMA system database that includes all data for scheduling, devices, dial rules, device registration, and site topology.
Logger.bak	The CMA system database for call detail records and gatekeeper diagnostic logs.
XMPP.bak	The CMA system database for presence information.

The following values are recommended for SQL server HD size:

Readimanager - 2GB with Autogrow

Logger - 4 GB with Autogrow

XMPP - 2 GB.

The Simple Recovery Model should be enabled for SQL backup mode.

Internal Databases

The CMA system automatically optimizes its internal database on an ongoing basis. It backs up its internal databases daily. The backup files are stored on the system's hard disk. The CMA system maintains the last four internal backups. To keep backups for a longer time period, copy them regularly to a different location. For more information, see [“Copy the CMA System Database Backup Files”](#) on page 428.

External Databases

You can integrate the CMA system to an external Microsoft SQL Server database. Some information about integrating with an external database:

- CMA systems with 400 or more registered endpoints and redundant systems require an external database.
- If you set up an external database, follow your own corporate policies (or Microsoft best practices) to back it up and maintain it. The CMA system does not back up its external databases.
- Anytime you switch from the internal CMA system database to an external Microsoft SQL Server database, some system configuration settings, for example the enterprise directory settings, must be reconfigured.
- Take steps to minimize database connection failures. For example:
 - Ensure you have good network connectivity between the CMA system and the Microsoft SQL Server. You may even consider co-locating the CMA system with your Microsoft SQL Server.
 - Increase the keep alive checks on the Microsoft SQL Server to once an hour.
- If your system does lose connection to the database, you must reboot the CMA system to restore login capability; the CMA system does not automatically reconnect to the database. For more information, see [“Restart or Shut Down a Polycom CMA System”](#) on page 6.
- It is recommended that anytime you reboot the external database server, you also restart the CMA system in the same maintenance window.
- You can create the CMA system databases manually using Microsoft SQL scripts. Contact Polycom Global Services to request the scripts.
- Anytime you switch from database sources (internal to external or external to internal), the default administrator's password is moved to the database as part of the switch.

Database Restoration

This section describes how to restore an internal CMA system database. To restore from an external Microsoft SQL Server databases, use Microsoft SQL Server Management Studio. Refer to your Microsoft SQL Server Management Studio documentation for more information.

You can migrate databases as follow.

From...	To...
Internal	Internal
Internal	External
External	External

When you restore internal or external databases:

- Do not allow users to connect to the server during the restoration process.
- Restore all of the system databases at the same time.
- Restore all of the system databases from backups that were taken at the same time.
- Restart the CMA system server when the restoration process is finished.

Database Operations

Before performing the database operations described here, Microsoft SQL Server should already be installed. (For information about the supported Microsoft SQL Server applications and service pack levels, see the *Polycom CMA System Release Notes* for the version you're running.)

The Microsoft SQL Server Setup wizard and documentation provides guidance for setting up Microsoft SQL Server. As you use the wizard, make these choices:

- For **Components to Install**, at a minimum choose the **SQL Server Database Services**.
- For **Instance Name**, select **Default Instance** and configure the database instance port (typically 1433).
- For **Service Account**, select the **Use the built-in System account** option.
- For **Authentication Mode**, select **Mixed Mode** and provide a password that meets your enterprise policy for password length and complexity.
- For **Collation Settings**, select **SQL collations**. The CMA system is only certified with the Microsoft SQL Server set to US-English Collation (SQL_Latin1_General_CP1_CI_AS).

- **Error and Usage Report Settings** are optional.

Integrate a Polycom CMA System to an External Database

To integrate a CMA system with an external database

- 1 Using the Microsoft SQL Server Configuration Manager, change the SQL Server keep alive checks (typically, **SQL Server 2005 Network Configuration > Protocols for MSSQLSERVER > TCP/IP > KeepAlive**) to 3,600,000 milliseconds.
- 2 At the CMA system interface, go to **Admin > Server Settings > Database**.
- 3 On the **Database** page, select **Use an external SQL Server database**.
- 4 Enter the **Database Server IP** address or **DNS Name**.
- 5 Enter the **Database Server Port** and click **Update**.
The system will guide you through formatting or upgrading the external database, as necessary.
- 6 Click **Finish**.

Revert a Polycom CMA System to its Internal Database

To revert a CMA system from an external database to its internal database

- 1 At the CMA system interface, go to **Admin > Server Settings > Database**.
- 2 On the **Database** page, clear **Use an external SQL Server database** and click **Update**.
- 3 Click **Update**.



Note

To go back to the external database, follow the procedure to [“Integrate a Polycom CMA System to an External Database”](#) on page 428.

Copy the CMA System Database Backup Files

In addition to backing up and restoring database files, you can copy the database backup files to and from the CMA system to an external location.

To copy the CMA system database backup files using the web interface

- 1 At the CMA system interface, go to **Admin > Database Backup Files**.
The **Database Backup Files** list appears showing all of the backup files stored on the CMA system. Files with a timestamp included in the name are system-generated backup files. Files without a timestamp are user forced backups.
- 2 In the **Database Backup Files** list, select the backup files of interest and click **Save**.
- 3 In the **Save As** dialog box, browse to a location and click **Save**.

Reformat the Existing Database

The CMA system has an option that allows you to completely reformat (clean out) the system's existing database.

IMPORTANT

Use this option only if your database is corrupted beyond repair or perhaps if you need to wipe out a test system to prepare it for production data.

To reformat the database, you must use the *PlcmDbo* user name and password during the process. This user name is an internal user name found at **Admin > Management and Security Settings > Database Security**. Be sure that you know the password for *PlcmDbo* before starting the reformat process.

By default, the password is not listed, but you can reset it. For more information, see [“Change Internal Database Passwords”](#) on page 461.

To reformat the existing databases

- 1 From the CMA system web interface, go to **Admin > Server Settings > Database**.
- 2 On the **Database** page, select **Reformat existing database...**
- 3 In the **Reformat Existing Database/Database Maintenance** dialog box, specify the **Database Server IP Address** and **Database Server Port Number** for the database to be reformatted.
- 4 Specify the *PlcmDbo* user **Login ID** and **Password** and click **Reformat/Install Database**.
- 5 Click **Yes** to confirm the reformat operation.

The system displays a **Reformat/Install Progress** bar to indicate that the system is reformatting the database.

Polycom CMA System Redundancy

This chapter describes how to configure a redundant Polycom® Converged Management Application™ (CMA®) system. It includes these topics:

- [Polycom CMA 5000 System Redundancy Overview](#)
- [Implement a Redundant Polycom CMA 5000 System](#)
- [License a Redundant Polycom CMA System](#)
- [Failover to a Redundant Polycom CMA 5000 System Server](#)
- [Discontinue Redundancy on a Polycom CMA 5000 System Configuration](#)

Polycom CMA 5000 System Redundancy Overview

A redundant CMA system configuration offers higher reliability and greater call success by ensuring that a CMA system server is always available.

A redundant CMA system configuration requires two CMA system servers and three IP addresses in the same subnet on the same network — one physical IP address for each of the servers and one virtual IP address dedicated to endpoint registration.

How Redundancy Works

Terminology is very important in understanding how redundancy works.

In a redundant configuration, one server is licensed as the *primary server* and the other server is licensed as the *redundant server*. The primary server is always the primary server and the redundant server is always the redundant server.

In a redundant configuration, there is only one *active server*. The active server is the server managing the system. It is the server running all of the CMA system services. In a normal operational state, the active server is the primary server. In a failover state, the active server is the redundant server.

In a redundant configuration, there is only one *standby server*. The standby server is the server that is not managing the system. It is the server running only the Polycom Service Monitor. In a normal operational state, the redundant server is the standby server. In a failover state, the active server is the standby server. (If at anytime you receive a *Cannot find server* error when you try to log into a server, check to see if it is the standby server.)

The Polycom Service Monitor monitors redundancy. In a normal operational state, the redundant/standby server sends a *SEND_REQUEST_STATUS* message via TCP every three seconds on port 700 to the primary/active server and expects the server to answer with a *SERVICE_RUNNING* message. (These messages do not include any qualitative data about the health of other services; they only verify that the active server is available on the network.)

If the redundant service sends three consecutive *SEND_REQUEST_STATUS* requests that go unanswered, its Service Monitor initiates a failover and the redundant server becomes the active server.

The most common reasons for system failovers are power failures and network disconnections. Note that failures in services do not initiate a failover, only a server failure.

If both the primary and redundant servers start simultaneously (for example if both are in the same location and recover from a power failure at the same time), both servers will initially attempt to become the active server. However, the redundant server – the server licensed as the redundant server – retreats to standby status once the system reaches its fully functional state.

An administrator can force a failover via the **Switch Server Roles** function in the CMA system user interface. Failover does not require a system restart.

The primary and redundant servers share the external CMA system database, so what is recorded by one CMA system is read by the other CMA system. An external Microsoft SQL Server database is required. The CMA system database information – call records, endpoint registration information, and network topology configurations – remains consistent and available during a failover because both servers point to the same database.

Also, the failover to the redundant server seems to occur seamlessly because the endpoints are registered with the virtual IP address, which remains constant.

During a failover:

- Active conferences are dropped from the system. Conference participants can call back in using the same conference information.
- Users logged into the CMA system user interface are disconnected during a failover and returned to the main CMA system web page. Users can log back in once the failover is completed.
- Users in the middle of an operation may get an error message, because the system is not available to respond to a request.

- The redundant server becomes the active server. Its services start in an order designed to prevent the new active server from being flooded with requests from endpoints during startup.

A system failover usually takes approximately 5 minutes, but some system settings affect how rapidly a redundant system returns to full functionality. The gatekeeper **Registration Refresh** period affects how quickly endpoints re-register with the redundant server after a failover. And if **Deny calls to/from unregistered endpoints** is checked, the gatekeeper rejects calls from endpoints that have not re-registered with the redundant server after a failover. Therefore, in a redundant system configuration, use a short refresh period (30 seconds) unless you have many endpoints or a large amount of network traffic.

Once a failover to a redundant server occurs, the redundant server manages all system operations until an administrator switches back to the original primary server via the **Switch Server Roles** function in the CMA system user interface.



Notes

- The CMA system does not automatically switch to the primary server when the primary server becomes available. An administrator must **Switch Server Roles**.
- A failover or system restart initiates an encryption routine that changes the private key for a redundant system. Therefore, after a failover or system restart, schedulers who use one of the scheduling plug-ins will be prompted to re-enter their login settings to access the system.

Redundant Configuration System Administration

Because the two servers share the external CMA system database, most of their configuration information is shared. However, certain information is not stored in the database, so an administrator must manually synchronize this information. This includes:

- Basic network settings such as IP, default gateway, and DNS settings
- External database information
- Time and external NTP server settings
- The current system log level
- Custom CMA system logo--upload the same logo to both servers
- Software Update profiles for scheduled software updates--upload the same software package to both servers

Whenever you change information in one of these sections on one server you should also change it on the other server.

Licensing and upgrading a redundant system is slightly more complex. The primary and redundant server required different licenses.

Implement a Redundant Polycom CMA 5000 System

You can set up a CMA 5000 system in a fault-tolerant, high-availability, redundant configuration. The CMA 4000 system is not available in a redundant configuration.

This section has two procedures. One describes how to convert an existing non-redundant CMA 5000 system to a redundant configuration. The other describes how to configure redundancy on a newly installed system.

To add a redundant Polycom CMA system server to an existing system

- 1 In a maintenance window when there are no running conferences, verify that your primary CMA 5000 system is pointed to an external Microsoft SQL Server database and is properly licensed.
- 2 Install the redundant CMA 5000 system as described in the *Polycom CMA Getting Started Guide*. During installation, point the redundant CMA 5000 system server to its internal database.
- 3 Request the required software activation key code for the redundant server as described in [“Request a Software Activation Key Code”](#) on page 411.
- 4 Enter the redundant license onto the redundant CMA 5000 system server.
 - a Log into the CMA 5000 system, and go to **Admin > Server Settings > Licenses**.
 - b Enter the activation key code for the redundant server into the **Add New License > Activation Key** field and click **Add**.

You will receive a message indicating that you’ve entered a redundant license and the system must be rebooted. DO NOT REBOOT NOW. The redundant server will automatically reboot when you perform step 6.
- 5 On the primary server:
 - a Go to **Admin > Server Settings > Redundant Configuration**.
 - b Enter the **Virtual IP** for the redundant system and click **Submit**.

The primary system will reboot.
- 6 Wait for the primary system to completely reboot and is back online, and then on the redundant server:
 - a Go to **Admin > Server Settings > Database**.
 - b On the **Database** page, select the **Use an external SQL Server database** check box.
 - c Enter the database information from the primary server that is, the database server’s IP address, and SQL server port number in the **Database** page.

d Click Update.

The CMA 5000 system connects to the database server and the redundant server restarts and comes online.

- 7** On the primary server, fail over to the redundant server. See [“Failover to a Redundant Polycom CMA 5000 System Server”](#) on page 437.

To configure redundancy on a newly installed Polycom CMA system.

A redundant CMA system configuration requires the installation of two CMA system servers on the same network. During **First Time Setup**, you are instructed to assign these two servers physical IP addresses and leave them pointed at their internal databases. This section describes how to complete the configuration of these newly installed redundant servers. It includes these topics:


- 1** [Configure the External Database for Redundancy](#)
- 2** [Set the Virtual IP Address for the Redundant System](#)

**Note**

This procedure describes implementing a new redundant CMA system. For information on converting an existing system to a redundant system, see [“Add or Remove a Polycom CMA System Custom Logo”](#) on page 412.

Configure the External Database for Redundancy


To configure the two redundant servers to use the same external database

- 1** Log into both the primary and redundant CMA 5000 system servers.
- 2** On the primary server, go to **Admin > Dashboard** and click **Shutdown**  to shut down the primary server.
- 3** When the primary server has shutdown completely, on the redundant server:

- a** Go to **Admin > Server Settings > Database**.
- b** On the **Database** page, select the **Use an external SQL Server database** check box.
- c** Enter the **Database Server IP** address or **DNS Name**.
- d** Enter the **Database Server Port** and click **Update**.

The system will guide you through formatting or upgrading the external database. The redundant server boots.

- e** After the redundant server restarts completely, log into it again and select **Admin > Dashboard**.

- f** Click **Shutdown**  to shut down the redundant server.
- 4** When the redundant server has shutdown completely, on the primary server:
 - a** Turn ON the primary server.
 - b** Log into the server and go to **Admin > Server Settings > Database**.
 - c** On the **Database** page, select the **Use an external SQL Server database** check box.
 - d** Enter the **Database Server IP** address or **DNS Name**.
 - e** Enter the **Database Server Port** and click **Update**.

The system will guide you through formatting or upgrading the external database. The primary server restarts and comes online as the active server.

Set the Virtual IP Address for the Redundant System

To set the virtual IP address for the redundant system

- 1** When the primary server has restarted completely, log into the primary CMA 5000 system server.
- 2** Go to **Admin > Server Settings > Redundant Configuration**.
If the two CMA system servers are installed and configured correctly on the network, both servers are displayed in the table on the **Redundant Configuration** page.
- 3** Enter the **Virtual IP** for the redundant system and click **Submit**. For information about this virtual IP address, see [“Add or Remove a Polycom CMA System Custom Logo”](#) on page 412.



Note

Set the virtual IP for the redundant server on the primary server only.


The primary server restarts and comes online as the active server.

- 4** When the primary server has restarted completely, turn ON the redundant server and wait for it to boot completely.

License a Redundant Polycom CMA System

To license a non-redundant CMA system, see [“Add Polycom CMA System Licenses”](#) on page 411. This topic describes how to license a redundant system.

To license a redundant CMA 5000 system

- 1 Request a separate software activation key code for the primary and redundant server as described in [“Request a Software Activation Key Code”](#) on page 411.
- 2 On the primary CMA 5000 system server:
 - a Go to **Admin > Server Settings > Database** and verify the database information. (If you fail to point the server to the correct database, you must re-enter the license when you change databases.)
 - b Go to **Admin > Server Settings > Licenses**.
 - c Enter the activation key code for the primary server into the **Add New License > Activation Key** field and click **Add**.
The license number appears in the list and the number of active licenses is updated.
 - d Go to **Admin > Server Settings > Redundant Configuration**, and click **Switch Server Role**.
The system fails over to the redundant server.
- 3 On the redundant server:
 - a Log into the CMA system *using the virtual IP address*, and go to **Admin > Server Settings > Licenses**.
 - b Enter the software activation key code for the redundant server into the **Add New License > Activation Key** field and click **Add**.
 - c Go to **Admin > Dashboard** and click **Restart**  to restart the system.
The system fails over to the primary server.

Failover to a Redundant Polycom CMA 5000 System Server

In a redundant configuration, the CMA 5000 system automatically fails over from the primary server to the redundant server. However, you can also manually initiate a failover.

To manually initiate a failover

- 1 On either server, go to **Admin > Server Settings > Redundant Configuration**.

- 2 On the **Redundant Configuration** page, click **Switch Server Role**.
The system initiates a failover to the other server.

Discontinue Redundancy on a Polycom CMA 5000 System Configuration

In some circumstances, you may need to discontinue redundancy. Use this procedure to do so, but only when the system is in a valid redundant state.

To discontinue a redundant Polycom CMA 5000 system configuration:

- 1 Log into the CMA 5000 system *using the virtual IP address*.
- 2 Failover to the redundant server. See [page 437](#).
- 3 On the redundant server:
 - a Go to **Admin > Server Settings > Database**.
 - b On the **Database** page, deselect the **Use an external SQL Server database** check box.
 - c Click **Update**.
The redundant server restarts.
- 4 On the primary server:
 - a Go to **Admin > Server Settings > Redundant Configuration**.
 - b On the **Redundant Configuration** page, click **Reset Redundant Configuration**.
The primary system restarts.

Gatekeeper Management

This chapter describes how to work with gatekeepers within the Polycom® Converged Management Application™ (CMA®) system. It includes these topics:

- [Primary Gatekeeper Management Operations](#)
- [Alternate Gatekeeper Management Operations](#)
- [Neighboring Gatekeeper Management Operations](#)

Primary Gatekeeper Management Operations

By default, the CMA system is made the primary gatekeeper during the **First Time Setup** process. Operations for managing the primary gatekeeper include:

- [Edit the Primary Gatekeeper Settings](#)
- [Configure Prefixed Based Registration](#)

Edit the Primary Gatekeeper Settings

To edit the primary CMA system gatekeeper settings

- 1 Go to **Admin > Gatekeeper Settings > Primary Gatekeeper**.
- 2 On the **Primary Gatekeeper** page, make the required changes.

The **Primary Gatekeeper Settings** include these fields:

Field	Description
Gatekeeper Identifier	The gatekeeper identifier (ASCII-only) on the network, which is used by the endpoints and CMA system for communication. The maximum number of characters is 254. All ASCII characters are valid.
Gatekeeper Description	The description (ASCII only) of this gatekeeper on the network.
Default Gatekeeper	When enabled, indicates that this CMA system is the default gatekeeper on the network.
Allow Registration of	Defines for the gatekeeper of which endpoints to allow to register. For more information, see “Device Registration” on page 396.
Registration Refresh (seconds)	The number of days that the CMA system gatekeeper maintains the endpoint registration information, in case the endpoint has not yet received any. The default is 30 days. Enter 999 to prevent endpoint registrations from expiring automatically.
Registration Refresh (seconds)	The interval at which the CMA system sends “keep-alive” messages to registered endpoints to determine whether they are online. The default is 300 seconds. If the endpoint responds with a registration request message, the endpoint is online. If not, the endpoint is offline. When the endpoint is registered to another gatekeeper, the CMA system still shows the endpoint’s status. To view the endpoint’s state (Online or Offline), go to Endpoint> Monitor View . Note Endpoints are Offline when they have been turned off or have been removed from the network. Endpoints return to an Online state when they have been turned on or have re-registered with CMA system.
Maximum Neighbor Gatekeeper Hop Counts	Limits the number of connections to make when an endpoint seeks dialing resolution. The default is 3.
Log calls to/from unregistered endpoints	Logs calls to and from rogue endpoints. To view call logs, select System Management > Reports > Gatekeeper Message Log .

Field	Description
Deny calls to/from unregistered endpoints	Prevents calls to and from rogue endpoints.
Enable Real-Time Statistics	Select this option to allow the gatekeeper to collect statistics from the endpoints.
IRR frequency	Specifies the interval (in seconds) at which endpoints that can report QoS (Quality of Service) measures will report them to the CMA system. By default, IRR is set to 0, which is equivalent to disabling the Real-time Statistics option. The valid IRR frequency range is 20 to 65535.
Call Model	Describes how the CMA system routes selected H.225 call signaling messages (that is, SETUP, CALL PROCEEDING, ALERTING, CONNECT, and NOTIFY message). Possible values include: Routed or Direct . For more information, see "Routing Mode" on page 398. In any case, Q.931 messages (ARQ, ACF, ARJ, BRQ, BCF, and BRJ) are always sent through the CMA system gatekeeper.

3 Click **Update**.

Configure Prefixed Based Registration

A user with administrator permissions can configure the CMA system so that only endpoints with specified E.164 prefixes are allowed to register to the H.323 gatekeeper.

Note that when you apply this policy to a system with existing endpoints, all existing endpoints that fail to meet the new policy will fail to re-register with the gatekeeper. This will be flagged in the **Endpoint > Monitor View** as a gatekeeper registration error.

To allow only the registration of endpoints with defined E.164 prefixes

1 Go to **Admin > Gatekeeper Settings > Primary Gatekeeper**.

On the **Primary Gatekeeper** page, change the **Allow Registration of** setting to **Predefined Prefixes Only**.

The **Valid E.164 Prefixes** entry box appears.

2 Enter a range of prefixes in the **From** and **To** fields and click **Add**.

The prefix range appears in the **Allowed Prefix Ranges** table.

- 3 Continue adding prefixes ranges as necessary. To delete a range, select the range and click the **Delete** button for it.

When you've specified all the prefix ranges, click **Update**.

Alternate Gatekeeper Management Operations

Alternate Gatekeeper Management Operations include:

- [Add an Alternate Gatekeeper](#)
- [Edit the Alternate Gatekeeper Settings](#)
- [Remove the Alternate Gatekeeper](#)

Add an Alternate Gatekeeper

To add an alternate gatekeeper

- 1 Go to **Admin > Gatekeeper Settings > Alternate Gatekeeper**.
- 2 On the **Alternate Gatekeeper** page, enter the required gatekeeper information.

The **Alternate Gatekeeper Settings** include these fields:

Field	Description
Need to Register	Check this box to require that a endpoint register with the alternate gatekeeper before sending other registration admission status requests. The default setting is unchecked.
Alternate Gatekeeper ID	The alternate gatekeeper's network identifier (ASCII only)
IP Address	The IP address of the alternate gatekeeper
Port	The port number (usually 1719) that the alternate gatekeeper uses to communicate with endpoints
Priority	Indicates the alternate gatekeeper's priority for endpoint registration. A lower number has higher priority (the range is 0 to 127), so endpoints would first register with an alternate gatekeeper with a priority of 0. The default setting is 0.

- 3 Click **Update**.

Edit the Alternate Gatekeeper Settings

To edit the alternate gatekeeper settings

- 1 Go to **Admin > Gatekeeper Settings > Alternate Gatekeeper**.
- 2 On the **Alternate Gatekeeper** page, make the required changes. For more information, see **Alternate Gatekeeper Settings**
- 3 Click **Update**.

Remove the Alternate Gatekeeper

To remove the alternate gatekeeper settings

- 1 Go to **Admin > Gatekeeper Settings > Alternate Gatekeeper**.
- 2 On the **Alternate Gatekeeper** page, clear the **Need to Register** check box.
- 3 Click **Update**.

Neighboring Gatekeeper Management Operations

Neighboring Gatekeeper Management Operations include:

- [View Neighboring Gatekeepers](#)
- [Add a Neighboring Gatekeeper](#)
- [Edit a Neighboring Gatekeeper](#)
- [Delete a Neighboring Gatekeeper](#)

View Neighboring Gatekeepers

To view the neighboring gatekeepers

- Go to **Admin > Gatekeeper Settings > Neighboring Gatekeepers**.

The **Neighboring Gatekeepers** list appears.

Column	Description
Name	The name of the region
Description	The description of the region

Add a Neighboring Gatekeeper

To add a neighboring gatekeeper

- 1 Go to **Admin > Gatekeeper Settings > Neighboring Gatekeeper**.
- 2 On the **Neighboring Gatekeeper** page, click **Add Neighbor**.
- 3 In the **Add Neighbor** dialog box, enter the required gatekeeper information and click **Save**.

The neighboring gatekeeper is added to the system.

Edit a Neighboring Gatekeeper

To edit the settings for a neighboring gatekeeper

- 1 Go to **Admin > Gatekeeper Settings > Neighboring Gatekeeper**.
- 2 On the **Neighboring Gatekeeper** page, select the neighboring gatekeeper of interest and click **Edit Neighbor**.
- 3 In the **Edit Neighbor** dialog box, make the required changes and click **Update**.
- 4 You'll need to reboot the CMA system to make the change effective.

Delete a Neighboring Gatekeeper

To delete a neighboring gatekeeper

- 1 Go to **Admin > Gatekeeper Settings > Neighboring Gatekeeper**.
- 2 On the **Neighboring Gatekeeper** page, select the neighboring gatekeeper of interest and click **Delete**.
- 3 Click **Delete** to confirm the deletion.

Management & Security Operations

This chapter describes the Polycom® Converged Management Application™ (CMA®) system management and security tasks. It includes these topics:

- [Update the Polycom CMA System Software](#)
- [Manage Certificates](#)
- [Change the System User Interface Timeout and Number of Sessions](#)
- [Give Enterprise Users Default Scheduler Role](#)
- [Change the Message for Enterprise Users without a Role](#)
- [Control Remote Desktop Connections to the CMA System](#)
- [Automatic Registration Synchronization](#)
- [Set Common Passwords for Endpoints](#)
- [Disable Common Password for Endpoints](#)
- [Set Local Account Lockout and Timeout](#)
- [Set Local Password Requirements](#)
- [Add Machine Accounts](#)
- [Change Internal Database Passwords](#)

Update the Polycom CMA System Software

To update a CMA system with a new software version, complete the following tasks:

- 1 Download the software upgrade file.
- 2 Obtain an upgrade key code.
- 3 Save a backup of the CMA system databases.
- 4 Perform the software upgrade.
- 5 Verify the upgrade.

For more information on performing each of these tasks, see the *Polycom CMA System Upgrade Guide*.

Manage Certificates

Certificates are a security technology that assists networked computers in determining whether to trust each other. Each digital certificate is identified by its public key. The collection of all public keys used in an enterprise to determine trust is known as a Public Key Infrastructure (PKI).

To manage digital certificates, an enterprise must:

- Establish a Public Key Infrastructure using one or more Certificate Authorities (CA). Typically, an enterprise's IT department has a CA but commercial CAs may be used as well.
- Configure each computer that participates in the PKI with a digital certificate that identifies it. The certificate must be signed by one of the CAs in the PKI
- Configure each computer that participates in the PKI to trust the PKI's Certificate Authorities
- Ensure that the PKI is used to protect data exchange by configuring each system to use encryption protocols such as Secure Sockets Layer (SSL) and/or Transport Level Security (TLS).

Certificates Accepted by the Polycom CMA System

By default, to support encrypted communications and establish a minimum level of trust, the CMA system presents a self-signed digital certificate to its clients. This default certificate will typically not be trusted by clients. Web browsers that connect to the CMA system user interface will display a warning regarding the certificate.

Participation in a Public Key Infrastructure requires a CMA system to have been configured with at least one root CA certificate, a current certificate revocation list (CRL) from the CA, and a digital certificate signed by the CA that identifies the CMA system.

Certificates come in several forms (encoding and protocol). The following table shows the forms that can be installed in the CMA system.

Encoding	Standard / File Type	Description and Installation Method
PEM (Base64-encoded ASCII text)	PKCS #7 standard P7B file	Certificate chain containing: <ul style="list-style-type: none"> • A signed certificate for the system, authenticating its public key. • The CA's public certificate. • Sometimes intermediate certificates. Upload file or paste into text box.
	CER (single certificate) file	Signed certificate for the system, authenticating its public key. Upload file or paste into text box.
	Certificate text	Encoded certificate text copied from CA's E-mail or secure web page. Paste into text box.
DER (binary format using ASN.1 Abstract Syntax Notation)	PKCS #12 standard PFX file	Certificate chain containing: <ul style="list-style-type: none"> • A signed certificate for the system, authenticating its public key. • A private key for the system. • The CA's public certificate. • Sometimes intermediate certificates. Upload file.
	PKCS #7 standard P7B file	Certificate chain containing: <ul style="list-style-type: none"> • A signed certificate for the system, authenticating its public key. • The CA's public certificate. • Sometimes intermediate certificates. Upload file.
	CER (single certificate) file (X.509 standard format)	Digital certificate that uniquely identifies the system within the PKI. Upload file.

Certificate Operations

In maximum security mode, the root CA certificate must be installed during First Time Setup. However, you can complete First Time Setup with just the root CA certificate and the CMA system default self-signed certificate. Then you can complete the process using the Certificate Management page.

In standard security mode, you can set up certificates at any time.

Use the Certificate Management page to:

- [View Certificates and Certificate Details](#)
- [Create a Certificate Signing Request](#)
- [Install a Certificate](#)
- [Upload a Certificate Revocation List](#)
- [Delete a Certificate](#)

View Certificates and Certificate Details

To view the list of installed certificates

- 1 Go to **Admin > Management and Security > Certificate Management**.

The **Certificate Management** page displays the list of currently installed certificates. By default, the system will display only one certificate. It will be identified as the *CMA server identity* certificate. When other certificates are installed, they will display along with the server identity certificate.

The **Certificate Management** page has this information.

Column	Description
Status	The status of the certificate. Possible values include: <ul style="list-style-type: none">• Certificate is valid• Certificate is invalid
Identifier	The certificate name as assigned by the CA

Column	Description
Purpose	<p>The type of certificate. Possible values are:</p> <ul style="list-style-type: none"> • CMA server identity—the system identity certificate. • Trusted root certificate—the root certificate for a CA. • Intermediate certificate—certificate from an intermediate CA. • Trusted peer—certificate from any server or computer that is not a CA but whose identity is trusted. The trusted peer certificate must be signed by one of the CAs installed in the CMA.
Expiration	The expiration date of the certificate.
CRL Next Update	<p>The date by which a new certificate revocation list from the CA must be uploaded.</p> <p>IMPORTANT</p> <p>If an administrator does not upload a new CRL by the CRL Next Update date, the system will become unresponsive. Recovering from this situation requires reinstalling from the recovery disk, manually reconfiguring of identity and root certificates, and restoring the system from a system backup.</p>

- 2 To view more information about a certificate, select the certificate and click **View Certificate Details**.

The **Certificate Details** dialog box appears with this information.

Section	Description
Certificate Info	Purpose and alias of the certificate.
Issued To	Information about the entity to which the certificate was issued and the certificate serial number.
Issued By	Information about the issuer.
Validity	Issue and expiration dates.
Fingerprints	SHA1 and MD5 fingerprints (checksums) for confirming certificate.
Public Key	The CMA public key, which in the public key system is distributed widely, and is not kept secure.
CRL Info	The date by which the current certificate revocation list must be replaced by a new list and the version of the list.

- 3 Use the arrows to reveal or hide information. Click **Close** when you are done.

Create a Certificate Signing Request

Although the initial CMA system configuration permits using the default, self-signed certificate, normal operation in a secure mode requires that you install a digital certificate signed by a trusted certificate authority that uniquely identifies the CMA system within your public key infrastructure. This can be done by creating a certificate signing request for the CMA system and submitting it to a certificate authority to be signed.



Note

Although it is common for a system to be identified by any number of digital certificates, each signed by a different CA, the CMA system currently only supports a single identity certificate.

This procedure describes how to create a certificate signing request (CSR) to submit to a certificate authority.

To create a certificate signing request

- 1 Go to **Admin > Management and Security > Certificate Management**.

The **Certificate Management** page displays the list of currently available certificates. By default, the system will have one server certificate identified as the *CMA server identity* certificate and one or more root certificates or certificate chains.

- 2 Click **Create Certificate Signing Request**.

If you see the warning “This action will overwrite any previously generated or uploaded private key. Do you want to continue?” do one of the following:

- If you are waiting for a previous request to be signed, click **No**. Because the CMA system currently supports only one identity certificate, only the most recent private key is retained. The digital certificate resulting from the most recent CSR is the only certificate that will match the retained private key and is therefore the only identity certificate that can be installed.
- If this is a new certificate signing request, click **Yes** to continue.

- 3 In the **Certificate Information** dialog box, enter the identifying information for your CMA system and click **OK**.

Field	Description
Country Name	Two-letter (ASCII only) ISO 3166 country code in which the server is located.
State or Province Name	Full state or province name (ASCII only) in which the server is located.
Locality Name	City name (ASCII only) in which the server is located.
Organization Name	Enterprise name (ASCII only) at which the server is located.
Organizational Unit Name	Subdivision (ASCII only) of the enterprise at which the server is located. Optional. Multiple values are permitted, one per line.
Common Name (CN)	The host name of the system (read-only), as defined in the network settings.
IPv4 Address	The IPv4 address of the system (read-only), as defined in the network settings.
IPv6 Address	When applicable, the IPv6 address of the system, as defined in the network settings.
Email Address	E-mail address (ASCII only) for a contact at the enterprise.

A **File Download** dialog box appears.

- 4 In the **File Download** dialog box, click **Save**.
- 5 In the **Save As** dialog box, enter a unique name for the file, browse to the location to which to save the file, and click **Save**.
- 6 Submit the file (or text within the file) as required by your certificate authority.

When your certificate authority has processed your request, it sends you a signed digital certificate for your CMA system. Some certificate authorities send only the signed digital certificate while others send all of the certificates that form the chain of trust (including intermediate and/or root CA certificates). These certificates may arrive as e-mail text, e-mail attachments, or be available on a secure web page.

Install a Certificate

This procedure describes how to install a certificate or certificate chain provided by a certificate authority. It assumes that you've received the certificate or certificate chain in one of the formats accepted by the CMA system. See ["Certificates Accepted by the Polycom CMA System"](#) on page 446.

**CAUTION**

Installing certificates requires a system restart and terminates all active conferences.

When you install a certificate, the change is made to the certificate store immediately, but the system can't implement the change until it restarts and reads the changed certificate store.

To install a signed certificate that identifies the CMA system

- 1 Go to **Admin > Management and Security > Certificate Management** and click **Install Certificates**.

A warning appears stating that changes made to the certificates will require a system restart to take effect.

- 2 In the **Add Certificates** dialog box, do one of the following:
 - If you have a PFX, P7B, or single certificate file, click **Upload certificate**, enter the password (if any) for the file, and browse to the file or enter the path and file name.
 - If you have PEM-format text, copy the certificate text, click **Paste certificate**, and paste it into the text box below. You can paste multiple PEM certificates one after the other.
- 3 Click **OK**.

If you are uploading a signed identity certificate for the first time, it will replace the CMA system self-signed certificate.
- 4 If you are uploading a signed identity certificate for the first time, you can verify that the new signed certificate has replaced the default self-signed certificate:
 - a In the list of certificates, select the *CMA server identity* certificate and click **View Certificate Details**.
 - b When the **Certificate Details** dialog box appears, verify that the information in the **Issued To** and **Issued By** sections has been replaced by the signed public certificate from the certificate authority.
 - c Click **OK** to close the dialog box.

**CAUTION**

The CMA 6.2 system requires certificates with Client and Server Authentication in the Enhanced Key Usage field, otherwise the certificate installation will fail.

Upload a Certificate Revocation List

This section describes how to install a certificate revocation list (CRL) provided by a certificate authority.

The CMA system requires a CRL for each CA or sub-CA in the certificate chain. The CMA system also requires that you upload a new CRL at regular intervals. This interval can be as short as a few days in higher security environments or a few months in environments with lower security requirements.



IMPORTANT

If an administrator does not upload a new CRL by the **CRL Next Update** date, the system will become unresponsive. Recovering from this situation requires reinstalling from the recovery disk, manually reconfiguring of identity and root certificates, and restoring the system from a system backup

To upload a certificate revocation list

- 1 Go to **Admin > Management and Security > Certificate Management** and click **Upload Certificate Revocation List**.
- 2 In the **Select file** dialog box, browse to the location of the CRL that you obtained from the CA and select the file.
- 3 Click **Open**.

Delete a Certificate

You can delete certificates from the CMA system, but the CMA system prevents you from deleting any certificate that breaks the identity certificate's chain of trust. To delete these certificates, new CA certificates must be installed and the identity certificate must be replaced.



Caution

Removing certificates requires a system restart, which terminates all active conferences.

When you remove a certificate, the change is made to the certificate store immediately, but the system can't implement the change until it restarts and reads the changed certificate store.

To delete a certificate

- 1 **Admin > Management and Security > Certificate Management.**
The **Certificate Management** page displays the list of currently available certificates.
- 2 Select the certificate to be deleted and click **Delete Certificate**.
A warning appears stating that changes made to the certificates will require a system restart to take effect.
- 3 Click **Yes** to continue.

- 4 When prompted, click **Yes** to confirm the deletion.

A dialog box informs you that the certificate has been deleted.

View the Expiration Dates for Certificates and CRLs

Certificates and certificate revocation lists expire. To view their expiration dates, see [“View Certificates and Certificate Details”](#) on page 448.

Change the System User Interface Timeout and Number of Sessions

To change the CMA system user interface timeout and number of sessions

- 1 Go to **Admin > Management and Security Settings > Session Management**.
- 2 On the **Session Management** page, configure these settings as needed.

Field	Description
CMA user interface timeout	By default, the CMA system user interface times out after 10 minutes of inactivity. Use this procedure to change the timeout value for the user interface inactivity timer. Possible value is 5 to 60 minutes.
Maximum number of sessions per user	The number of simultaneous login sessions per user ID. By default, the maximum number of sessions per user ID is 5. Possible value is 1 to 10 sessions.
Maximum number of sessions per system	<p>The number of simultaneous login sessions by all users. By default, the maximum number of sessions by all users is 50. Possible value is 2 to 50 sessions.</p> <p>Note</p> <p>If this limit is reached, but none of the logged-in users is an Administrator, the first Administrator user to arrive is granted access, and the system terminates the non-Administrator session that's been idle the longest.</p>

- 3 Click **Update**.

Give Enterprise Users Default Scheduler Role

By default when local users are added to the CMA system, they are assigned the **Scheduler** role. By default, when you integrate a CMA system to an Active Directory, enterprise users are not assigned a role. In this case, you must either assign each enterprise user a role, or you can use this procedure to give enterprise users the **Scheduler** role by default.

To give enterprise users default Scheduler role for a Polycom CMA system

- 1 Go to **Admin > Management and Security Settings > Session Management**.
- 2 Select the **CMA access via default profile allowed** option.
- 3 Click **Update**.

Change the Message for Enterprise Users without a Role

To change the message enterprise users without a role see when they try to log into a Polycom CMA system

- 1 Go to **Admin > Management and Security Settings > Session Management**.
- 2 Edit the **Message to be displayed to unauthorized users**.

For example, enter a message such as "Your username and password are valid, but you have no permissions on this system. Contact your IT department for more information."
- 3 Click **Update**.

Control Remote Desktop Connections to the CMA System

By default, users can access the CMA system using the Windows Remote Desktop Connection. You can disable this ability.

To control CMA system access with Remote Desktop Connection

- 1 Go to **Admin > Management and Security Settings > Session Management**.
- 2 Clear the **Enable remote desktop connections** option.
- 3 Click **Update**.

Automatic Registration Synchronization

You can configure the CMA system to send registration server addressing information for the gatekeeper and/or global directory server (GDS) when the endpoint is registered to the CMA system.



Note

For the CMA system, the GDS is the same as the global address book (GAB).

This automatic registration synchronization service only works for endpoints that register with the gatekeeper or GDS or are manually added to the CMA system after the **Automatic Registration Synchronization** setting is enabled.

So if the **Automatic Registration Synchronization** setting is enabled and an endpoint registers with the gatekeeper, the gatekeeper addressing information is sent to the endpoint. If the **Automatic Registration Synchronization** setting is enabled and an endpoint registers with the GDS, the GDS addressing information is sent to the endpoint. If the **Automatic Registration Synchronization** setting is enabled and an endpoint is added manually to the CMA system, both the gatekeeper and GDS addressing information is sent to the endpoint.

If automatic discovery and configuration is not successful, you can manually add endpoints.



Notes

- **Automatic Registration Synchronization** works only for endpoints that register with the gatekeeper or Global Directory Server after the setting is enabled; it does not automatically register pre-existing endpoints.
- The CMA system only supports Automatic Registration Synchronization for Polycom and selected third-party endpoints operating in standard mode. For supported endpoint types, including third-party endpoint types, see [“Endpoint Types”](#) on page 87.

To enable Automatic Registration Synchronization of endpoints

- 1 Go to **Admin > Management and Security Settings > Endpoint Management Settings**.
- 2 In the **Automatic Registration Synchronization** section of the **Endpoint Management Settings** page, select **Synchronize endpoint registration** and click **Update**.

After you have changed this setting, all endpoints you add are automatically provisioned.

Set Common Passwords for Endpoints

The **Common Password** feature allows you to manage endpoints that have the same global administrative password. However, it cannot reset the administrative password on endpoints.

If you use the **Common Password** feature, access to password-protected data within endpoints is granted if the specified common password matches the endpoints' **Administrator Password**.

To set common passwords for endpoints

- 1 Go to **Admin > Management and Security Settings > Endpoint Management Settings**.
- 2 In the **Common Password** section of the **Endpoint Management Settings** page, select **Use a Common Password**.
- 3 Enter the common **User Name** and the common password in the **Password** and **Verify Password** fields and click **Update**.



Note

Leave these settings blank if your Polycom endpoints require individual passwords or do not have passwords. To configure a global administrative password for all Polycom endpoints, use scheduled provisioning.

Disable Common Password for Endpoints

To disable common passwords for endpoints

- 1 Go to **Admin > Management and Security Settings > Endpoint Management Settings**.
- 2 In the **Common Password** section of the **Endpoint Management Settings** page, clear **Use a Common Password** and click **Update**.

The common password feature is disabled. However, the values for the common password feature are retained in the database, so it can be easily re-enabled.

Set Local Account Lockout and Timeout

To set local account lockout and timeout

- 1 Go to **Admin > Management and Security Settings > Local User Account Configuration**.
- 2 On the **Local User Account Configuration** page, configure these settings as needed.

Field	Description
Account Lockout	
Failed login threshold	Specify how many consecutive login failures cause the system to lock an account. Possible value is 2 to 10.
Failed login window (hours)	Specify the time span within which the consecutive failures must occur in order to lock the account. Possible value is 1 to 24.
Customized user account lockout duration (minutes)	Specify how long the user's account remains locked. Possible value is 1 to 480.
Account Inactivity	
Customize account inactivity threshold (days)	Specify the inactivity threshold that triggers disabling of inactive accounts. Possible value is 30 to 180.

- 3 Click **Update**.

Set Local Password Requirements

The **Local Password Requirements** page allows users assigned the **Administrator** role to change, but not disable password, security requirements by specifying password age, length, and complexity.

To set local password requirements

- 1 Go to **Admin > Management and Security Settings > Local Password Requirements**.

- 2** On the **Local Password Requirements** page, configure these settings as needed.

Field	Description
Password Management	
Minimum length (characters)	Specify the number of characters a password must contain. Possible value is 8 to 18.
Minimum changed characters	Specify the number of characters that must be different from the previous password. Possible value is 1 to 4.
Minimum password age (days)	Specify how frequently a password can be changed. Possible value is 1 to 30.
Maximum password age (days)	Specify at what age a password expires. Possible value is 30 to 180.
Password warning interval (days)	Specify when users start to see a warning about their password expiration. Possible value is 1 to 7.
Reject previous passwords	Specify how many of the user's previous passwords the system remembers and won't permit to be reused. Possible value is 8 to 16.
Password Complexity	
Lowercase letters	Specify the number of lowercase letters (a-z) that a password must contain. Possible value is 1 or 2.
Uppercase letters	Specify the number of uppercase letters (A-Z) that a password must contain. Possible value is 1 or 2.
Numbers	Specify the number of digit characters (0-9) that a password must contain. Possible value is 1 or 2.
Special characters	Specify the number of non-alphanumeric keyboard characters that a password must contain. Possible value is 1 or 2.
Maximum consecutive repeated characters	Specify how many sequential characters may be the same. Possible value is 1 to 4.

- 3** Click **Update**.

Add Machine Accounts

For dynamically managed endpoints associated with a room, a user assigned the **Administrator** role must associate each room in the CMA system with a machine account. The machine account allows the room's endpoint to connect and authenticate with the CMA system for directory and dynamic management purposes without using the endpoint user's account.

You can setup the room and machine account the following ways:

- You can set up a machine account and create a new room at the same time, then edit the room to complete the room information.
- You can create a new room, then create the machine account and associate the machine account with the existing room. For more information, see [“Add a Local Room”](#) on page 344.

In a maximum security environment, dynamically managed HDX systems also require a machine account for each HDX that the CMA system will manage. The machine account allows the endpoint to connect and authenticate with the CMA system for dynamic management purposes without using the endpoint user's account.

The **Add Machine Account** dialog box includes the following information.

Field	Description
Enable Machine Account	Select or clear this option to enable and disable (respectively) the machine account you create for the endpoint.
Unlock Machine Account	Select this option to unlock machine accounts that become locked when they exceed the Failed login threshold. This will only happen when the password expires.
User ID	Enter a unique name for the machine account. As a best practice, name the machine account in a way that associates it with the corresponding device. For example, if your company names endpoint systems for the system user or room (for example, <i>bsmith_HDX</i> or <i>Evergreen_Room</i>), then give the machine account an associated User ID (<i>bsmith_HDX_machine</i> or <i>evergreen_room_machine</i>).
Password/ Confirm Password	Enter a password for the machine account user ID. This password must meet the Local Password Requirements . This password expires in 365 days.

Field	Description
Description	Enter a meaningful description for the endpoint.
Associate with an existing user or room	Select this option to associate the endpoint system with a specific user or room. This may be a local or enterprise user or room.
Associate with a new room (created automatically)	Select this option to associate the endpoint system with a system-generated room. The name of the new room is the same as the machine account User Name and can be edited when you edit the room.

Once you have created this machine account on the CMA system, provide this information to the appropriate HDX system administrator. They should enter this **User ID** and **Password** as the **User Name** and **Password** on the HDX **Provisioning Service** page.

Note that the machine account password expires after one year. After the expiration, the HDX login will fail. After three failed login attempts, the system locks the machine account. You can reset the password and unlock the machine account by editing it and assigning a new password.

To add a machine account

- 1 Go to **Admin > Management and Security Settings > Machine Accounts**.
- 2 Click **Add**.
- 3 In the **Add Machine Account** dialog box, complete the fields.
- 4 Click **OK**.

Change Internal Database Passwords

The CMA system uses three user names to access internal databases. You can change the passwords for those user names to comply with any requirements you may have to change passwords on a regular basis.

You also use the user listed as PlcmDbo if you should need to reformat your internal database. For more information, see [“Reformat the Existing Database”](#) on page 429.

The system will restart after you change these passwords. Make sure that you use this function when no conferences are active or scheduled.

To change internal database passwords

- 1 Go to **Admin > Management and Security Settings > Database Security**.

- 2** Select the database user whose password you want to change.
- 3** Click **Change Password**.
- 4** In the Change Database User Password dialog, enter the new password in the **New Password** and **Confirm New Password** fields.

If you want the system to generate a password, click **Create Password**. Be sure to write down the password that displays.
- 5** Click **OK**.
- 6** Click **Apply Password Changes**.

The system resets the passwords and restarts. It may take the CMA system up to 10 minutes to shut down and then restart all server processes.

Dial Plan Setup Operations

This chapter describes how to edit the default Polycom CMA system Dial Plan settings to support your company's site topology. It includes these topics:

- [Site Operations](#)
- [Site Link Operations](#)
- [Site-to-Site Exclusions](#)
- [Territories](#)
- [Network Clouds](#)
- [Dial Plan Service Operations](#)
- [Dial Rule Operations](#)
- [Least-Cost Routing Operations](#)
- [E.164 Numbering Scheme](#)

Site Operations

Site operations include:

- [View the Graphical Site Topology](#)
- [View the Sites List](#)
- [Add a Site](#)
- [View Site Information](#)
- [Assign Locations to a Site](#)
- [Edit Site Settings](#)
- [Edit Site Provisioning Settings](#)
- [Delete a Site](#)

View the Graphical Site Topology

To view the graphical site topology

- Go to **Admin > Dial Plan and Sites > Site Topology**.

The **Site Topology** page appears. It graphically displays the sites and site links defined to the CMA system.

- Hover over a map element to view information about it.
- Use the slider bar to zoom in or out on the map.
- Select or deselect elements (**Site Links**, **Bandwidth**, or **Site Names**) to change what is displayed on the map.
- Use the **Select Sites** drop-down list to filter (by site name, territory name, IP address, network devices, and alerts) which sites are displayed on the map.

View the Sites List

To view the Sites list

- Go to **Admin > Dial Plan and Sites > Sites**.

The **Sites** list appears. It includes this information:

Column	Description
Name	Name of the site.
Description	Description of the site.
Country Code	The country code for the country in which the site is located.
Area Code	The city or area code for the site. Do not include a leading zero. For example, the city code for Paris is 01; however, enter 1 in this field.
Max Bandwidth (Mbps)	The total bandwidth limit for audio and video calls.
Max Bit Rate (Kbps)	The per-call bandwidth limit for audio and video calls.
Territory	The territory to which the site belongs, which determines the CMA system responsible for it.

Add a Site

To add a site

- 1 Go to **Admin > Dial Plan and Sites > Sites** or **Admin > Dial Plan and Sites > Site Topology**.
- 2 In the **Sites** list or **Site Topology** page, click **Add Site**.
- 3 In the **Add Site** dialog box, enter a **Site Name** and **Description** for the site.
- 4 Complete the **General Info**, **Routing**, **Subnet**, and if applicable **ISDN Number Assignment**, sections of the **Add Site** dialog box. The minimum information required is **Site Name**, **Description**, **Location**, and **Subnets**.
For information about all of the site fields, see [“Add/Edit Site Dialog Box”](#) on page 388.

- 5 Click **OK**.

The new site is added to the system and the **Edit Site Provisioning** dialog box appears. These are the site-based parameters that the CMA system automatically provisions to endpoint systems operating in dynamic management mode.

- 6 As needed, edit the default site provisioning details and click **Apply**.



Note

Not all of the site provisioning parameters apply to all endpoint systems being provisioned. If an endpoint system does not have a corresponding parameter, it ignores the parameter.

Field	For the endpoint systems at the site being provisioned...
Date and Time Settings	
Country	Specify the country code for their location.
Date Format	Specify the date display format.
Auto Adjust for Daylight Saving Time	Specify whether or not to adjust the endpoint's system clock for daylight savings time.
Time Format	Specify the time display format.

Field	For the endpoint systems at the site being provisioned...
Time Server	<p>Specify whether to connect to a time server for automatic system time settings.</p> <p>Select Auto to require that the video endpoint system synchronize with an external time server that is identified by a network domain controller. Because it is identified by a network domain controller, you do not need to enter the IP address of the time server.</p> <p>Select Manual to require that the video endpoint system synchronize with an external time server that may not be identified by a network domain controller. In this case, you must also enter the IP address of the time server in the Time Server Address field.</p> <p>If Time Server is set to Off, or if the Time Server is set to Manual or Auto but the endpoint system cannot connect to the time server, the date and time must be manually reset at the endpoint.</p>
Primary Time Server Address	Specify the address of the primary time server when Time Server is set to Manual .
Secondary Time Server Address	Specify the address of the secondary time server when Time Server is set to Manual .
Timezone	Specify the time difference between GMT (Greenwich Mean Time) and the endpoint system's location.
Firewall Settings	
Use Fixed Ports	<p>Specify whether to define the TCP and UDP ports.</p> <ul style="list-style-type: none"> If the firewall is H.323 compatible or the endpoint systems are not behind a firewall, disable this setting. If the firewall is not H.323 compatible, enable this setting. The endpoint systems will assign a range of ports starting with the TCP and UDP ports you specify. The endpoint system defaults to a range beginning with port 3230 for both TCP and UDP. <p>Note</p> <p>You must open the corresponding ports in the firewall. You must also open the firewall's TCP port 1720 to allow H.323 traffic.</p>
Start TCP Port	<p>Lets you specify the beginning value for the range of TCP ports used by the endpoint systems. The endpoint systems will automatically assign a range of ports starting with the port you specify.</p> <p>Note</p> <p>You must also open the firewall's TCP port 1720 to allow H.323 traffic.</p>
Start UDP Port	Lets you specify the beginning value for the range of TCP ports used by the endpoint systems. The endpoint systems will automatically assign a range of ports starting with the port you specify.
Enable H.460 Firewall Traversal	Allows the endpoint system to use H.460-based firewall traversal. For more information, see the <i>Administrator's Guide for Polycom HDX Systems</i> .

Field	For the endpoint systems at the site being provisioned...
NAT Configuration	Specify whether the endpoint systems should determine the NAT Public WAN Address automatically. <ul style="list-style-type: none"> If the endpoint systems are behind a NAT that allows HTTP traffic, select Auto. If the endpoint systems are behind a NAT that does not allow HTTP traffic, select Manual. Then specify a NAT Public (WAN) Address. If the endpoint systems are not behind a NAT or are connected to the IP network through a virtual private network (VPN), select Off.
NAT Public (WAN) Address	When NAT Configuration is set to Manual , specify the address that callers from outside the LAN should use to call the endpoint systems.
NAT is H.323 Compatible	Specify that the endpoint systems are behind a NAT that is capable of translating H.323 traffic.
Address Displayed in Global Directory	Specify whether to include the endpoint system's information in the global directory <ul style="list-style-type: none"> Select Private to exclude the endpoint from the global directory Select Public to include the endpoint in the global directory
H323 Settings	
Enable IP H.323	Specify whether to enable IP H.323 calls.
Use Gatekeeper	When IP H.323 is enabled, Specify whether the endpoint systems will use the CMA system as its gatekeeper or another gatekeeper. Gateways and gatekeepers are required for calls between IP and ISDN. <ul style="list-style-type: none"> This Server — The endpoint systems will use the CMA system as their gatekeeper. Specify — The endpoint systems will use another system as their gatekeeper.
Gatekeeper IP Address	When Use Gatekeeper is set to Specify , enter the gatekeeper IP address in this field.
Use Gatekeeper for Multipoint Calls	Specify whether multipoint calls use the endpoint system's internal multipoint capability or the Polycom MCU's Conference on Demand feature. This feature is available only if the system is registered with a PathNavigator or CMA system gatekeeper.
SIP Settings	
Enable SIP	Specify whether to enable SIP calls.
Automatically Discover SIP Servers	The CMA system will issue a DNS query to locate the SIP server and provision that information to endpoints.
Proxy Server	Specify the IP address or DNS name of the SIP proxy server for the network.
Registrar Server	Specify the IP address or DNS name of the SIP registrar server for the network. <ul style="list-style-type: none"> In an Microsoft Office Communications Server 2007 or Microsoft Lync Server 2010 environment, specify the IP address or DNS name of the Office Communications Server or Lync Server server. If registering a remote HDX system with an Office Communications Server Edge Server or Lync Server Edge Server, use the fully qualified domain name of the access edge server role.
Backup Proxy Server	Specify the IP address or DNS name of a backup SIP proxy server for the network.

Field	For the endpoint systems at the site being provisioned...
Backup Registrar Server	Specify the IP address or DNS name of a backup SIP registrar server for the network
Transport Protocol	<p>Indicates the protocol the system uses for SIP signaling. The SIP network infrastructure determines which protocol is required.</p> <ul style="list-style-type: none"> • Auto enables an automatic negotiation of protocols in the following order: TLS, TCP, UDP. This is the recommended setting for most environments. • TCP provides reliable transport via TCP for SIP signaling. • UDP provides best-effort transport via UDP for SIP signaling. • TLS provides secure communication of the SIP signaling. TLS is available only when the system is registered with a SIP server that supports TLS. When you choose this setting, the system ignores TCP/UDP port 5060..
SIP Server Type	Specify whether the SIP registrar server is a Microsoft Office Communications Server or a Microsoft® Lync™ Server 2010. Enabling this setting activates integration features such as the Microsoft global directory and Office Communicator contact sharing with presence.
Verify Certificate	Enable this option when the endpoint system's certificate should be verified by the certificate authority.
Use Enterprise Credentials	Enable this option when the endpoint system should use the credentials the user entered at the endpoint to use for authentication when registering with a SIP registrar server.
User Name	Specify the name to use for authentication when registering with a SIP registrar server, for example, <i>msmith@company.com</i> . If the SIP proxy requires authentication, this field and the password cannot be blank.
Password	Specify the password that authenticates the system to the registrar server.
Provisioning Settings	
Provisioning Polling Interval (minutes)	<p>Specify the frequency at which the endpoint systems poll the CMA system for new provisioning information.</p> <p>By default, this interval is 60 minutes. For performance reasons, the minimum positive value for this interval is 5 minutes. There is no maximum value enforced. When the value of this interval is set to 0, the endpoint systems do not poll the CMA system for new provisioning information.</p>
Software Update Polling Interval (minutes)	<p>Specify the frequency at which the endpoint systems poll the CMA system for a new software update package.</p> <p>By default, this interval is 60 minutes. For performance reasons, the minimum positive value for this interval is 5 minutes. There is no maximum value enforced. When the value of this interval is set to 0, the endpoint systems do not poll the CMA system for a new software update package.</p>
Quality of Service Settings	
Video Type of Service Value	Specify the IP Precedence or Diffserv value for video packets.
Audio Type of Service Value	Specify the IP Precedence or Diffserv value for audio packets.

Field	For the endpoint systems at the site being provisioned...
FECC Type of Service Value	Specify the IP Precedence or Diffserv value for Far End Camera Control packets.
Type of Service Field	Specify the service type and the priority of IP packets sent to the system for video, audio, and far-end camera control: <ul style="list-style-type: none"> • IP Precedence — Represents the priority of IP packets sent to the system. The value can be between 0 and 5. • Diffserv — Represents a priority level between 0 and 63. If this setting is selected, enter the value in the Type of Service Value field.
Maximum Transmission Unit Size (bytes)	Specify the Maximum Transmission Unit (MTU) size used in IP calls. If the video becomes blocky or network errors occur, packets may be too large; decrease the MTU. If the network is burdened with unnecessary overhead, packets may be too small; increase the MTU.
Enable PVEC	Allows the endpoint system to use PVEC (Polycom Video Error Concealment) if packet loss occurs. PVEC delivers smooth, clear video over IP networks by concealing the deteriorating effects of packet loss
Enable RSVP	Allows the endpoint system to use Resource Reservation Setup Protocol (RSVP) to request that routers reserve bandwidth along an IP connection path. Both the near site and far site must support RSVP in order for reservation requests to be made to routers on the connection path.
Enable Dynamic Bandwidth	Specify whether to let the endpoint system automatically find the optimum line speed for a call.
Maximum Transmit Bandwidth (Kbps)	Specify the maximum transmission line speed.
Maximum Receive Bandwidth (Kbps)	Specify the maximum reception line speed.
Security Settings	
Security Profile	Read-only field. Displays the security level of the CMA system.
Use Room Password for Remote Access	Specify whether the local endpoint system password and remote access password are the same.
Room Password	Enter or change the local endpoint system password here. When the local password is set, you must enter it to configure the system Admin Settings using the remote control. The local password must not contain spaces.
Administrator ID	Enter the administrative account that should be used to access the endpoint system remotely.
Remote Access Password	For endpoint systems, enter or change the remote access password here. When the remote access password is set, you must enter it to upgrade the software or manage the endpoint systems from a computer. The remote access password cannot include spaces.

Field	For the endpoint systems at the site being provisioned...
Meeting Password	<p>Specify the password users must supply to join multipoint calls on this endpoint system if the call uses the internal multipoint option, rather than a bridge.</p> <p>This field can also be used to store a password required by another endpoint system that this system calls. If a password is stored in this field, you do not need to enter it at the time of the call; the endpoint system supplies it to the system that requires it. The meeting password cannot include spaces.</p>
Enable Secure Mode	<p>Specify whether to operate in secure mode (also known as security mode), which uses TLS, HTTPS, AES, digital signatures, and other security protocols, algorithms, and mechanisms. These protocols encrypt management communication over IP, preventing access by unauthorized users.</p> <p>When devices at a site are provisioned to operate in secure mode, the CMA system can only perform the dynamic management operations of automatic provisioning, automatic software update, and directory and presence services for the devices. The CMA system cannot perform monitoring or control operations for the devices.</p> <p>For more information, see the <i>Administrator's Guide for Polycom HDX Systems</i>.</p>
AES Encryption	<p>Specify how to encrypt calls with other sites that support AES encryption.</p> <ul style="list-style-type: none"> • Off—No encryption is used. • When Available—AES Encryption is used with any endpoint that supports it, even if the other endpoints in the call don't support it. • Required for Video Calls Only—AES Encryption is used for all video endpoints in the call. Analog phone and voice over ISDN connections are allowed. Video endpoints must support AES Encryption to participate in the call. • Required for All Calls—AES Encryption is used for all video endpoints in the call. Analog phone and voice over ISDN connections are not allowed. All endpoints must support AES Encryption to participate in the call.
Enable Web Access	<p>Specify whether to allow remote access to the endpoint system by the web.</p> <p>Note</p> <p>The endpoint systems will restart if the remote access settings are changed. This setting does not deactivate the associated port, only the application. Use the Web Access Port setting to disable the port.</p>
Enable Telnet Access	<p>Specify whether to allow remote access to the system by Telnet.</p> <p>Note</p> <p>The endpoint systems will restart if the remote access settings are changed. This setting does not deactivate the associated port, only the application. Use the Web Access Port setting to disable the port.</p>
Enable SNMP Access	<p>Specify whether to allow remote access to the system by SNMP.</p> <p>Note</p> <p>The endpoint systems will restart if the remote access settings are changed. This setting does not deactivate the associated port, only the application. Use the Web Access Port setting to disable the port.</p>

Field	For the endpoint systems at the site being provisioned...
Web Access Port	<p>Specify the port to use when accessing the endpoint system's web interface.</p> <p>If you change this from the default (port 80), specify a port number of 1025 or higher, and make sure the port is not already in use. You will need to include the port number with the IP address when you use the Polycom HDX web interface to access the system. This makes unauthorized access more difficult.</p> <p>Note</p> <p>The system restarts if you change the web access port.</p>
Allow Video Display On Web	<p>Specify whether to allow viewing of the room where the endpoint system is located, or video of calls in which the endpoint system participates, using the endpoint system's web interface.</p> <p>Note</p> <p>This feature activates both near site and far site video displays in Web Director.</p>
NTLM Version	Specify the NTLM version the endpoint system should use to authenticate.
Security Settings 2	
Idle Session Timeout in Minutes	When sessions are enabled, Specify the number of minutes your system can be idle before the session times out.
Lock Port after Failed Logins	<p>Specify the number of failed login attempts allowed before the system locks the account. If set to Off, the system will not lock the user account due to failed login attempts.</p> <p>This selection controls local and web interface login attempts. For example, if you select 3 here, a user who fails to log in properly twice on the web interface and twice on the local interface is locked out on the fourth attempt.</p>
Failed Login Window in Hours	Specify the amount of time that the account remains locked due to failed login attempts.
Port Lock Duration in Minutes	Specify the amount of time that the port remains locked due to failed login attempts.
Maximum Peer Certificate Chain Depth	Specify how many links a certificate chain can have. The term peer certificate refers to any certificate sent by the far-end host to the HDX system when a network connection is being established between the two systems.
Verify Certificates for all Web Access	Specify whether the endpoint requires certificate validation to access the endpoint.
Whitelist	
Enable Whitelist of IPs	When a whitelist is enabled, allows access to an endpoint's web interface only by those systems with an IP address that matches a pattern using regular expression notation.

Field	For the endpoint systems at the site being provisioned...
Enter all IPs allowed to Connect via the web	<p>Specify (by IP addresses using regular expression notation) which systems can access an endpoint's web interface. Addresses are matched by pattern, which means that you could allow IP address that you did not mean to allow. For example, if you entered an IP address of 15.1.2.111, all of the following results would match:</p> <ul style="list-style-type: none"> • 15.1.2.111 • 15.182.1.11 • 15.1.252.111 <p>If you want to allow a range of IP addresses, use the * wildcard instead. For example, enter 10.11.*.* to allow all IP addresses that begin with 10.11.</p>
General Settings	
Heartbeat Posting Interval (minutes)	Specify the frequency at which the endpoint systems poll the CMA system for a heartbeat.
In Call Stats Posting Interval (minutes)	Specify the frequency at which the endpoint systems poll the CMA system for in call statistics.
Calendar Settings	
Automatically Discover Exchange Server	Specify that the CMA system should discover the Microsoft Exchange server for the site by searching DNS records.
Specify Exchange Server	Specify that the CMA system should use the Microsoft Exchange server specified in the Exchange Server Address field.
Exchange Server Address	Specify the IP address or DNS name of the Microsoft Exchange server for the site.
LDAP Settings	
Group Display Name	Specify whether the CMA system should identify groups by their common name (cn) or their DisplayName. These names are extracted from the Active Directory.
User Display Name	Specify whether the CMA system should identify users by their common name (cn) or their DisplayName. These names are extracted from the Active Directory.
Enterprise Directory Admin Group	Specify the Active Directory group whose members should have access to the Admin settings on the HDX system. This name must exactly match the name in the Active Directory server for authentication to succeed.
Enterprise Directory User Group	Specify the Active Directory group whose members should have access to the User settings on the HDX system. This name must exactly match the name in the Active Directory server for authentication to succeed.

View Site Information

To view information about an existing site

- 1 Go to **Admin > Dial Plan and Sites > Sites** or **Admin > Dial Plan and Sites > Site Topology**.
- 2 In the **Sites** list or **Site Topology** page, select the site of interest and click **Site Information**.

The **Site Information** dialog box displays the following site information.

Column	Description
Name	Name of the site.
Description	Description of the site.
Location	The specified location of the site identified either by longitude + latitude or by country + city.
Bandwidth (Mbps)	The specified total bandwidth limit for audio and video calls.
Bandwidth Used	Identifies the percentage of the maximum bandwidth currently occupied with audio and video calls.
Device Types	Identifies the type (Bridges, DMAs, VBPs, and Endpoints) and number of devices assigned to the site.
Alarms	Identifies the device alarms present within the site. Alarm information includes Status, Device Name, Device Type, and Description. Click Details to view more device details.
Subnets	Identifies the subnets within the site. Subnets information includes Bandwidth Used, Subnet (name), and (maximum) Bandwidth.

Assign Locations to a Site

Location has not always been a required field for sites. If your existing sites do not include location information, use the **Assign Locations** action to update your sites.

To assign a location to an existing site

- 1 Go to **Admin > Dial Plan and Sites > Sites** or **Admin > Dial Plan and Sites > Site Topology**.
- 2 Click **Assign Locations**.

- 3** In the **Assign Locations to Sites** dialog box, select the site of interest and click **Specify Location**.
- 4** To specify a location by city name:
 - a** From the **Enter Location By** drop-down list, select **Search for City**.
 - b** If you know it, select the **Country** name for the location.
 - c** Enter the name of the **City** and click **Search**.

The system returns the list of cities that match your entry.
 - d** Select the appropriate city using the **Country**, **Division**, and **Subdivision** fields to identify it and click **Select**.
- 5** To specify a location by latitude and longitude in decimal degrees format:
 - a** From the **Enter Location By** drop-down list, select **Latitude/Longitude (Decimal format)**.
 - b** Enter the **Latitude** and **Longitude** coordinates in decimal degrees (for example, Baltimore has a latitude of 39.3° and a longitude of 76.6°).
 - c** Enter a **Location Name**. The system uses this location name for reference only; it does not validated the location name against the latitude and longitude coordinates that you enter.
 - d** Select the **Country** name for the location and click **Select**.

The system uses the coordinates you input to place the site in the proper location on its site topology map.
- 6** To specify a location by latitude and longitude in DaysMinutesSeconds format:
 - a** From the **Enter Location By** drop-down list, select **Latitude/Longitude (DDD:MM:SS format)**.
 - b** Enter the **Latitude** and **Longitude** coordinates in the required format and select
 - c** Enter a **Location Name**. The system uses this location name for reference only; it does not validated the location name against the latitude and longitude coordinates that you enter.
 - d** Select the **Country** name for the location and click **Select**.

The system uses the coordinates you input to place the site in the proper location on its site topology map.

Edit Site Settings



Note

Changing network topology may affect the accuracy of reports based on this information. To retain historical data for the current network topology, generate reports before making changes.

To edit settings for a site

- 1 Go to **Admin > Dial Plan and Sites > Sites** or **Admin > Dial Plan and Sites > Site Topology**.
- 2 In the **Sites** list or **Site Topology** page, select the site of interest and click **Edit Site**.
- 3 Edit the **General Info**, **Site Routing**, **Site Subnet**, and if applicable **ISDN Number Assignment**, sections of the **Edit Site** dialog box. For information about these sections, see [“Add/Edit Site Dialog Box”](#) on page 388.
- 4 Click **OK**.

Edit Site Provisioning Settings

To edit the site provisioning settings for a site

- 1 Go to **Admin > Dial Plan and Sites > Sites** or **Admin > Dial Plan and Sites > Site Topology**.
- 2 In the **Sites** list or **Site Topology** page, select the site of interest and click **Edit Site Provisioning Details**.
- 3 As needed, edit the site provisioning details and click **Apply**. For information about these details, see [“Add/Edit Site Dialog Box”](#) on page 388.
- 4 Click **OK**.

Delete a Site



Note

Devices that belonged to a deleted site are automatically reassigned to support Internet and VPN calls.

To delete a site

- 1 Go to **Admin > Dial Plan and Sites > Sites** or **Admin > Dial Plan and Sites > Site Topology**.
- 2 In the **Sites** list or **Site Topology** page, select the site of interest and click **Delete**.
- 3 Click **Yes** to confirm the deletion.

Set Up SIP

The CMA system supports SIP to establish conference connections. If you want to use SIP, you must enable it and configure SIP settings. You must also upload SIP URI data.

To implement SIP, complete the following tasks

- 1 Configure the SIP settings for each site.

When you add a site to the CMA system, you also set up site provisioning, which includes the SIP settings. Be sure to enable SIP and configure the servers, protocol, and credentials needed for your SIP server. See [“Add a Site”](#) on page 465.

- 2 Import SIP URI data.

After you enable and configure SIP, you must import your endpoint SIP data from your SIP server. The import provides the CMA system with all of the URI data it needs to use SIP.



Note

If you are using Microsoft as your SIP server, you do not need to import SIP URI data. The CMA system can retrieve the SIP URI from the enterprise directory.

- a Create a CSV file in the format described here. The import requires a CSV file in the following format:

domain,username,deviceType,URI

where:

- » *domain*—Specifies the domain the user uses to log in to the CMA system.
- » *username*—Specifies the CMA system user name.
- » *deviceType*—Specifies the device type (valid values are HDX, VVX, and CMADesktop).
- » *URI*—Specifies the SIP URI for this user.

For example:

local,johndoe,HDX,johndoe@example.com

- b From the CMA system, go to **Admin > Uploads**.
- c Click **Upload**.
- d Navigate to the CSV file, select it, and click **Open**.

Whenever you add new users or rooms or need change a SIP URI, you must provide SIP URI data. For the methods available for editing the SIP URI, see [“Edit SIP URI Data”](#) on page 477.

Edit SIP URI Data

You can edit SIP URI data in the following ways:

- Upload a CSV file that has changes or new data.
 - Data in the CSV file is added to any existing data.
 - For information about the CSV file format and the upload process, see [“Set Up SIP”](#) on page 476.
- Edit individual users or rooms.
 - For each CMA system user or room, you can add or edit the SIP URI in the **Dial String Reservations** section of the **Edit User** or **Edit Room** dialog box.

Site Link Operations

When you add a site link, you enter the starting and ending sites of the link and the maximum bandwidth and bit rates available for calls (audio and video) that use the link. Links are bidirectional. After you have created a link from Site A to Site B, you automatically have a bi-directional link from Site B to Site A, although the link appears as unidirectional.



Note

The bit rate can be set at the network level, the device level, and the conference level. If there is a discrepancy between these bit rate settings, the system implements the lowest bit rate setting. The only exception, is that the bit rate in the RMX profile takes precedence over the bit rate in the conference settings.

Field	Description
Name	Name (ASCII only) of the inter-site link.
Description	Description (ASCII only) of the inter-site link.
From Site	Identifies the first site to be linked. The drop-down list includes all defined sites and the Internet.
To Site	Identifies the other site to be linked. The drop-down list includes all defined sites and an Internet/VPN option.
Total Bandwidth (kbps)	The maximum available bandwidth for audio and video calls, which you set at the gateway or router.
Call Max Bit Rate (kbps)	The maximum bit rate allowed for an audio and video call.

Site-link operations include:

- [View the Site Links List](#)
- [Add a Site Link](#)
- [Edit a Site Link](#)
- [Delete a Site Link](#)

View the Site Links List

To view the Site Links list

- Go to **Admin > Dial Plan and Sites > Site-Links**.

The **Site-Links** list appears.

Column	Description
Name	Name of the link
Description	Description of the link
From Site	First site reached in the call route
To Site	Final site reached through this call link
Max Bandwidth	The maximum available bandwidth for audio and video calls, which you set at the gateway or router. Only applies to direct links.
Max Bit Rate (kbps)	The maximum bit rate allowed for an audio and video call. Only applies to direct links.

Add a Site Link

Before you can create a site link, you must add two or more sites to the system.

To add a site link

- 1 Go to **Admin > Dial Plan and Sites > Site-Links**.
- 2 In the **Site-Links** page, click **Add**.
- 3 In the **Add Site-Link** dialog box, enter a **Name** and **Description** for the link and select the starting (**From Site**) and ending (**To Site**) sites.
- 4 Enter the **Bandwidth** and **Max Bit Rate** and click **Save**.

The new link appears on the **Site Links** page.

Edit a Site Link

You may need to edit site links when network changes are made.

If you make a bandwidth change, the current load is not affected; however, the bandwidth available for future conferences may be affected.

To edit a site link

- 1 Go to **Admin > Dial Plan and Sites > Site-Links**.
- 2 In the **Site-Links** list, select the link of interest and click **Edit**.
- 3 In the **Edit Site-Link** dialog box, edit the **Name**, **Description**, **Bandwidth** or **Max Bit Rate**.
- 4 Click **Save**.

Delete a Site Link

You can remove site links from the Polycom CMA system.

**Note**

Avoid removing a link on which a scheduled conference depends.

To delete a site link

- 1 Go to **Admin > Dial Plan and Sites > Site-Links**.
- 2 In the **Site-Links** list, select the site link of interest and click **Delete**.
- 3 Click **Yes** to confirm the deletion.

Site-to-Site Exclusions

Create site-to-site exclusions to explicitly deny connection between two sites for audio or video calls.

Site-link exclusion operations include:

- [View the Site-to-Site Exclusion List](#)
- [Add a Site-to-Site Exclusion](#)
- [Edit a Site-to-Site Exclusion](#)
- [Delete a Site-to-Site Exclusion](#)

View the Site-to-Site Exclusion List

To view the Site-to-Site exclusion list

- Go to **Admin > Dial Plan and Sites > Site-to-Site Exclusion**.
The **Site-to-Site Exclusions** list appears.

Add a Site-to-Site Exclusion

Before you can create a site link exclusion, you must add two or more sites to the system.

Exclusions are by definition bilateral. No call traffic is allowed to flow across the site-link in either direction.

To add a site-to-site exclusion

- 1** Go to **Admin > Dial Plan and Sites > Site-to-Site Exclusions**.
- 2** In the **Site-to-Site Exclusions** page, click **Add**.
- 3** In the **Add Site-to-Site Exclusions** wizard:
 - a** Select the first site of the **From/To** site pair (by clicking the appropriate button). If needed, use the **Search Site** field to find the site.
 - b** Select the second site of the **From/To** site pair (by enabling the appropriate check box) and click **Continue**. You can select more than one site, if needed.
 - c** Review the site-to-site exclusion and if it is correct, click **Save Exclusion**.

Edit a Site-to-Site Exclusion

You cannot edit a site-to-site exclusion; you can only delete it and then re-add it.

Delete a Site-to-Site Exclusion

To delete a site-to-site exclusion

- 1** Go to **Dial Plan and Sites > Site-to-Site Exclusions**.
- 2** In the **Site-to-Site Exclusions** page, select the exclusion of interest and click **Delete**.
- 3** Click **Yes** to confirm the deletion.

Territories

A territory is a set of one or more sites for which a CMA system is responsible. By default, there is one territory named **Default CMA Territory**, and its primary node (the CMA system responsible for it) is set to this system. For more information, see [“Territories”](#) on page 393.

Territory operations include:

- [View the Territory List](#)
- [Add a Territory](#)
- [Edit a Territory](#)
- [Delete a Territory](#)

View the Territory List

To view the Territories list

- Go to **Admin > Dial Plan and Sites > Territories**.
The **Territories** list appears.

Add a Territory

To add a territory

- 1 Go to **Admin > Dial Plan and Sites > Territories**.
- 2 In the **Territories** page, click **Add**.
- 3 Complete the **Territory Info** and **Associated Sites** sections of the **Add Territories** dialog box. For information about these fields, see [“Add/Edit Territory Dialog Box”](#) on page 393.
- 4 Click **OK**.

Edit a Territory

To edit a territory

- 1 Go to **Admin > Dial Plan and Sites > Territories**.
- 2 In the **Territories** page, select the territory of interest and click **Edit**.

- 3 Change the **Territory Info** and **Associated Sites** information of the **Add Territories** dialog box as needed. For information about these fields, see [“Add/Edit Territory Dialog Box”](#) on page 393.
- 4 Click **OK**.

Delete a Territory

To delete a territory

- 1 Go to **Admin > Dial Plan and Sites > Territories**.
- 2 In the **Territories** page, select the territory of interest and click **Delete**.
- 3 Click **Yes** to confirm the deletion.

Network Clouds

To simplify the network topology, define network clouds to represents a hub with many sites connected to each other such as a private network or VPN.

Network cloud operations include:

- [View the List of Network Clouds](#)
- [Add a Network Cloud](#)
- [Edit a Network Cloud](#)
- [Delete a Network Cloud](#)

View the List of Network Clouds

To view the Territories list

- Go to **Admin > Dial Plan and Sites > Territories**.
The **Territories** list appears.

Add a Network Cloud

To add a network cloud

- 1 Go to **Admin > Dial Plan and Sites > Network Clouds**.
- 2 In the **Network Clouds** page, click **Add**.

- 3** In the **Cloud Info** section of the **Add Network Cloud** dialog box, enter a unique and meaningful **Name** and **Description** for the cloud.
- 4** To create a link between a site and the network cloud:
 - a** Click **Linked Sites**.
 - b** In the **Search Sites** field, enter all or part of the site name or location and click **Find**.

The list of sites containing the search phrase appear in the **Search Results** column.
 - c** Select one or more sites to link with the network cloud and then click the right arrow to move them to the **Selected Sites** column.
- 5** Click **OK**.

Edit a Network Cloud

To edit a network cloud

- 1** Go to **Admin > Dial Plan and Sites > Network Clouds**.
- 2** In the **Network Clouds** page, select the network cloud of interest and click **Edit**.
- 3** Edit the **Cloud Info** or to create a link between a site and the network cloud:
 - a** Click **Linked Sites**.
 - b** In the **Search Sites** field, enter all or part of the site name or location and click **Find**.

The list of sites containing the search phrase appear in the **Search Results** column.
 - c** Select one or more sites to link with the network cloud and then click the right arrow to move them to the **Selected Sites** column.
- 4** Click **OK**.

Delete a Network Cloud

To delete a network cloud

- 1** Go to **Admin > Dial Plan and Sites > Network Clouds**.
- 2** In the **Network Clouds** page, select the network cloud of interest and click **Delete**.
- 3** Click **Yes** to confirm the deletion.

Dial Plan Service Operations

Dial plan services are special features that video endpoint system users can invoke by dialing the prefix assigned in the CMA system to that service.

The CMA system has two default dial plan services:

- [Conference on Demand](#)
- [Simplified Dialing](#)

These services can be edited and disabled, but not deleted.

You can also add other gateway or If a service does not appear automatically when a device registers with the CMA system, you can define the service manually so that it is available for video endpoint system users. In addition, you can add services for certain third-party MCU services.

Conference on Demand

With Conference on Demand, video endpoint system users can start an unscheduled multipoint conference from their endpoint rather than requesting this service from an administrator.

The initiating endpoint uses the capabilities made available through the MCU. When Conference on Demand is enabled on the endpoint, the CMA system sends the call directly to the MCU.



Note

Conference on Demand is only available on Polycom RMX and MGC MCUs. It is not available on Polycom RMX 1000 MCUs.

The following table provides details on how the Conference on Demand service is configured.

Field	Description
General Info	
Service Type	Conference on Demand (read only)
Enable	Indicates whether or not the service is enabled
Available for New Groups	Indicates whether or not the service is available for new user groups
Description	Description (ASCII only) of the service. By default for this service, Conference on Demand
Service Prefix	The prefix (ASCII only) for the service. By default for this service: con

Field	Description
Conference on Demand—MCU Properties	
Login ID	User login (ASCII only) for the MCU hosting the conference. This user account must be authorized to create new conferences.
Password	Password (ASCII only) for the user login. Each time you modify the password for the MCU, you must also modify it in this page.
H.323 Network Service	The corresponding service created on the MCU to implement this CMA system service. Set on the MCU (ASCII only).
Default Conference Properties	
MGC: Video Session	Indicates what users see. Set to Continuous Presence for this service. Notes <ul style="list-style-type: none"> MGC only. For RMX MCUs, the profile determines this setting. Select Transcoding to support IP and ISDN calls.
MGC: Bit rate (Kbps)	Default bit rate for calls. Notes <ul style="list-style-type: none"> MGC only. The RMX MCU bit rate is dictated by the RMX profile. The video endpoint system that starts the Conference on Demand call may use a higher or lower bit rate than is specified in this page.
RMX: Profile Name	The name of the RMX profile that has the conference settings for the conference.

Simplified Dialing

Simplified dialing is a service that allows video endpoint system users to access gateway services by dialing 9, and then the phone number or other dialing string. Simplified dialing is enabled by default.

To use simplified dialing, the following settings are also required:

- Sites must specify the country code, city and area code, and number of digits in the subscriber line.
- The gateway must be registered with the CMA system and display in the **List of Devices** page.
- Gateway services must be defined.
- The LCR table must be defined.

Field	Description
Service Type	Name of the service (read only)
Enable	Indicates whether this service is enabled
Available for New Groups	The service is available for new user groups
Description	Description of the service
Service Prefix	The prefix for this service: 9.

Gateway Service

These services are provided by a gateway to endpoints. For example, gateways usually have distinct services for each speed they support (128 Kbps, 384 Kbps, 512 Kbps, and so on) and a service for audio-only calls.

Gateway services tell the CMA system how to route the call during conversion between IP and ISDN.



Note

Gateway and MCU services must be defined in both the CMA system and the MCU platform. They must be defined exactly the same in both locations. If you enter this information manually, be sure to type it exactly as it is entered in the MGC or RMX system.

You can simplify entry of services by making sure that the MCUs and gateways on your video conferencing network are set to register with the gatekeeper in the CMA system. This setting assures the information appears automatically in the **List of Services** page.

You must define a gateway service for each bit rate available. These services should appear automatically in the list when the gateway registers with the CMA system. If gateway services do not appear, you can enter them manually. If the **List of Services** page does not include gateway services, alternate routing and least-cost routing are disabled. For details, see the following table.

Field	Description
Service Type	Type of service
Enable	Indicates whether this service is enabled
Available for New Groups	The service is available to new user groups
Description	Description of the service
Service Prefix	The prefix for this service. Must be a registered E.164 alias for the corresponding gateway in the Devices page for Directory Setup .

Field	Description
For use in simplified dialing	
Device Capability	<p>Specify the type of connection the device can handle. Select all that apply. Options are:</p> <ul style="list-style-type: none"> • H.320. Supports video and voice using the ITU H.320 standard. • Voice. Supports voice over the PSTN network. • Other. Supports a protocol other than H.320 or voice, such as H.321 or video over ATM.
Bit Rate (Kbps)	<p>The maximum rate at which the calls can connect.</p> <p>Note</p> <p>If you select Unknown, this service cannot support simplified dialing.</p>
Insert between prefix and first number	<p>Specify the character to insert in the dial string between the prefix and the first number.</p> <p>For example, if you specify * as the character, the sequence the user enters would be:</p> <p>77*2125551212</p>
Insert between phone number	<p>Specify the character to insert in the dial string between phone numbers.</p> <p>For example, if you specify # as the character to separate numbers, the sequence the user enters would be:</p> <p>77*5551212#5651213</p>
Append after full dial string	<p>Specify the character to append after the full dial string.</p> <p>To process the call, certain gateways require a symbol be appended after the final dialing number.</p> <p>For example, if you specify ** as the characters to append after the final dialing number, the sequence the user enters would be:</p> <p>77*5551212#5651213#2223232**</p> <p>Warning: The CMA system does not recognize dial strings that require termination after the ISDN number and have an extension after the terminated ISDN.</p> <p>For example, the CMA system does not recognize the following dial string:</p> <p>165024710000**3452</p>

MCU Service

These services allow devices to use specific MCU features and settings when making a call. For example, an MCU can define a service for a multipoint video call with continuous presence at 384 Kbps and another service for video switching at 256 Kbps.

MCU services and their associated prefixes are defined at the MCU. For MGC or RMX MCUs, the MCU services should appear automatically in the **List of Services** page when the MCU registers with the CMA system. Because third-party MCUs may not automatically register, you must enter them manually in the CMA system.

Use MCU services to dial the IP gateway segment that translates between IP and ISDN, in conference calls with two or more participants, or continuous presence.

Field Name	Description
Service Type	Type of service.
Enable	Indicates whether this service is enabled or not.
Available for New Groups	The service is available for new user groups.
Description	Description of the service. To identify it easily in the List of Services page, include the prefix and the MCU feature (for example, 384 K video switching).
Service Prefix	The prefix for this service, which must be a E.164 alias that is registered for the MCU on the Device page.

Services operations include:

- [View the Services List](#)
- [Add a Service](#)
- [Edit a Service](#)
- [Delete a Service](#)

View the Services List

This page shows the services that have been defined in your dial plan. These services are available when you place unscheduled calls.



Note

E.164 aliases appear in this list as follows:

- For MGC and RMX devices, they appear as gateway services.
- For a device's H.323 services, they (including the alias prefix) appear as MCU services. Gateway service prefixes are the E.164 aliases of the MCU's gateway session profiles.

To view the Services list

- Go to **Admin > Dial Plan > Services**.

The **Services** list appears.

Column	Description
Prefix	Prefix of the service.
Type	The type of service. Available types include System, Gateway, and MCU.
Description	Description of the service. Tip: When completed automatically, the description reflects the value entered in the MGC or RMX manager.
Enabled	By default, services are enabled. To disable them, clear the Enabled check box.

Add a Service

If a gateway or MCU service does not appear automatically when the device registers with the CMA system, you can define the service manually so that it is available for use in unscheduled calls. In addition, you can add services for certain third-party MCU services.

To add a service

- 1 Go to **Admin > Dial Plan > Services**.
- 2 In the **Services** list, click **Add Service**.
- 3 Complete the **General Info**, and if applicable **Simplified Dialing** or **Conference on Demand**, sections of the **Add Service** dialog box.

- 4 Click **OK**.

The new service is added to the system.

Edit a Service

You can make changes to a service.



Note

Be sure that the information you enter in the CMA system matches the information entered in the MCU.

To edit a service

- 1 Go to **Admin > Dial Plan > Services**.
- 2 In the **Services** list, select the service of interest and click **Edit Service**.
- 3 As required, edit the **General Info**, and if applicable **Simplified Dialing** or **Conference on Demand**, sections of the **Edit Service** dialog box.
- 4 Click **OK**.

Delete a Service

You can delete a gateway or MCU service from the CMA system. You cannot delete the **Conference on Demand** or **Simplified Dialing** service.

To delete a service

- 1 Go to **Admin > Dial Plan > Services**.
- 2 In the **Services** list, select the service of interest and click **Delete Service**.
- 3 Click **Yes** to confirm the deletion.



Notes

- The system returns an error message if you attempt to delete any services that were added automatically when the MCU registered with the CMA system. To avoid this, first unregister and then delete the MCU.
- MCU services added manually from the **Services** page are not affected by this error.

Dial Rule Operations

Dial rules describe how the CMA system gatekeeper should resolve addresses in an incoming dial string to route a call. This dial string may include an IP address, a string of numbers that begin with a prefix associated with a service, a string that begins with a country code and city code, or a string that matches a particular alias for a device.

Dial strings may match multiple dial rules. However, you can assign a priority to each dial rule. When the CMA system gatekeeper receives a call request and associated dial string, it reviews the dial rules in order of priority. The first matched (highest priority) dial rule is executed.

Field	Description
General Info	
Name	Name (ASCII only) of the dial rule.
Description	Description (ASCII only) of the dial rule, which can be up to 256 characters long.
Priority	Priority number of the dial rule, which determines which rule the CMA system uses first. The smaller the number the higher the priority. More than one dial rule may have the same priority. In that case, rules with the same priority are applied in random order.
Enabled	Select the check box to enable the rule.
Pattern Type	Specify the type of pattern to be matched. Available patterns include: <ul style="list-style-type: none"> Local Directory Services DNS Name IP Address Prefix Prefix Range
Applicable Site	Site to which this pattern applies. You can select a specific site or all sites. This field is not available when the Pattern Type is Local Directory Services .
Routing Action > Dial String Manipulation	
IP Address Pattern Data	Specify the criteria (ASCII only) to use to match the pattern type and additional changes to make when routing the call. This field is available when the Pattern Type is DNS Name , IP Address , or Prefix . This field is not available when the Pattern Type is Local Directory Services or Prefix Range .

Field	Description
Start Value	The starting number to use as a prefix, which displays only for rules with the Prefix Range pattern type.
End Value	The ending number to use as a prefix, which displays only for rules with the Prefix Range pattern type
# Characters to remove	Number of digits to remove (from the start or from the end) of the dialed string This field is available when the Pattern Type is Local Directory Services , Prefix , and Prefix Range . This field is not available when the Pattern Type is DNS Name or IP Address .
Prefix to add	Prefix to add to the dialed string This field is available when the Pattern Type is Local Directory Services , Prefix , and Prefix Range . This field is not available when the Pattern Type is DNS Name or IP Address .
Routing Action > Action to perform	
Action	Specify what action to take for calls that match the pattern type and criteria. Action to perform when the pattern is matched. Depending on the Pattern Type , options may include: <ul style="list-style-type: none"> • Route • Block • Route within region • Route out of region • Route to a gateway with LCR applied • Route to a gateway service • Route to a list of gateway services • Route to a trusted neighbor
Trusted Neighbors	
Available Region	When the action is Route to a trusted neighbor , select the region to which you want to route.
Gateway Services	
Selected Gateway Services (prioritized)	When the action is Route to a gateway service , this field lists the selected gateway services. You can define multiple gateway services for a rule. The first in the list is the default gateway service. Others are used in priority order when the primary gateway service is not available.

Default Dial Rules

The CMA system has three default dial rules. With these defaults, the system can route most calls except those requiring an external DNS lookup.

- **Internal IP** - This dial rule allows the system to identify the incoming dial string as an IP addresses and routes the call out of the region. By default, this dial rule applies to all sites.
- **Alias** - This dial rule allows the system to identify the incoming dial string as belonging to the local directory and routes the call to the local device or service, as required.
- **DNS Name** - This dial rule allows the system to identify the incoming dial string as a DNS name and block the call.



Note

Do not delete the default dial rules or the CMA system will not be able to route calls correctly. You can disable a dial rule by editing it and clearing the **Enabled** check box for the rule.

Parts of a Dial Rule

A dial rule consists of a pattern type paired with a routing action. When the dialed string uses a pattern that matches the pattern type, the associated rule is applied.

Pattern Types

A pattern type tells the CMA system how to find a match for the dial string. The following table shows the available pattern types.

Pattern Type	Description
Local Directory Services	Search the List of Devices and List of Services . Includes aliases, which are searched before the service prefix.
DNS Name	Look up a DNS Name
IP Address	Look for an IP addresses in the IPV4 format
Prefix	Look for a prefix specified in the dial rule
Prefix Range	Look for a prefix within the range of prefixes specified in the dial rule

Routing Actions

A routing action informs the CMA system what to do based on the dial rule's associated pattern type. The following table shows the available routing actions.

Routing Action	Pattern Type	Description
Route	All	Allow the call to pass
Block	All	Block the call
Route within region	IP Address	Route to any IP address inside the region
Route out of region	IP Address	Route to any IP address outside the region Note The originating site's Internet access rules still apply.
Route to a gateway with LCR	Prefix and Prefix Range	Remove the prefix specified in the dial rule and route the remaining dial string to a gateway service, which has the specified LCR table
Route to a gateway service	Prefix and Prefix Range	Remove the prefix specified in the dial rule and route the remaining dial string to the specified gateway service
Route to a list of gateway services	Prefix and Prefix Range	Modify the dial string specified in the dial rule and route the remaining dial string to the specified gateway service.
Route to a trusted neighbor	Prefix and Prefix Range	Modify the dial string as specified in the dial rule and ask the specified neighboring gatekeeper to route the modified dial string. If the neighboring gatekeeper agrees, route the call. Note The neighboring gatekeeper must be configured as a region in the CMA system.

Examples of Custom Dial Rules

You use custom dial rules to perform these tasks:

- **Block calls.** For example, you can block all calls to 900 numbers, which usually charge a per-minute fee. Create a dial rule with these settings:
 - Pattern type: Prefix
 - Prefix to match: 900
 - Routing action: Block

- **Route to a neighboring gatekeeper.** If you have entered information about neighboring gatekeepers in the **List of Regions** page, you can create a rule to route calls to another gatekeeper. Create a dial rule with these settings:
 - Pattern type: Prefix Range
 - Prefixes to match: Specify the range.
 - Routing action: Select **Route to a trusted neighbor** and the region for the neighboring gatekeeper to which you want to route calls.
- **IP-specific routing.** You can specify which calls may connect, according to the IP address. For example, you could allow calls from San Jose to Atlanta, but not from San Jose to Pleasanton.

Dial Rule operations include:

- [View the Dial Rules List](#)
- [Add a Dial Rule](#)
- [Enable or Disable Dialing Rules](#)
- [Edit a Dial Rule](#)

View the Dial Rules List

To view the Dial Rules list

- Go to **Admin > Dial Plan > Dial Rules**.

The **Dial Rules** list appears.

Column	Description
Name	The name of the dial rule
Pattern Type	<p>The pattern type in use for this rule. Options are:</p> <ul style="list-style-type: none"> • Local Directory Services • DNS Name • IP Address • Prefix • Prefix Range <p>For more information, see “Parts of a Dial Rule” on page 494.</p>
Pattern Data	Additional criteria that must be met to apply this rule

Column	Description
Routing Action	<p>The routing action used by this rule. Options are:</p> <ul style="list-style-type: none"> • Route • Block • Route within region • Route out of region • Route to a GW with LCR applied • Route to a GW service • Route to a list of GW services • Route to a trusted neighbor <p>Note Not all actions are available for all pattern types.</p>
Site	The sites for which this rule is used. May be all sites or a specific site
Priority	The priority assigned this rule
Enabled	Indicates whether or not the dial rule is enabled

Add a Dial Rule

To add a dial rule

- 1 Go to **Admin > Dial Plan > Dial Rules**.
- 2 In the **Dial Rules** list, click **Add Dialing Rule**.
- 3 Complete the **General Info**, **Routing Action**, **Trusted Neighbors**, and **Gateway Services** sections of the **Add Dialing Rule** dialog box.
- 4 Click **OK**.

The new dial rule is added to the system.

Enable or Disable Dialing Rules

You can enable or disable dial rules.



Note

Use caution when changing the default dial rules, which enable basic operations in the CMA system.

To enable or disable a dialing rule

- 1 Go to **Admin > Dial Plan > Dial Rules**.
- 2 In the **Dial Rules** list, select the dial rule of interest and click **Edit Dialing Rule**.
- 3 On the **Dial Rules - General Information** page, check or clear the **Enabled** check box.
- 4 Click **OK**.

Edit a Dial Rule

To edit a dial rule

- 1 Go to **Admin > Dial Plan > Dial Rules**.
- 2 In the **Dial Rules** list, select the dial rule of interest and click **Edit Dial Rule**.
- 3 In the **Edit Dial Rule** dialog box, make the required changes.
- 4 When you are finished, click **OK**.

Least-Cost Routing Operations

Least-cost routing (LCR) allows the CMA system to route ISDN or POTS calls made on paths that incur the lowest expense. You can route calls from one site through a gateway in another site by referencing LCR tables.

Least-cost routing is useful when sites already have a high-bandwidth connection between them.

Least-cost routing works with the CMA system's other routing features.

Setting up least-cost routing requires you to:

- Determine the LCR information to enter in the CMA system.
- Create LCR tables.
- In the device record for MCUs:
 - Define an H.320 service and select the LCR table to use.
 - Define a gateway service and select the H.320 service associated with the LCR table.

**Note**

Make sure the LCR tables you define match the network setup.

You cannot use least-cost routing when:

- The route cannot be identified.
- The required resources are unavailable.
- Bandwidth limitations exist on the WAN.

How Least-Cost Routing Works

Each LCR table defines dial strings, which include the country code, area code, prefix, and a weighted cost for commonly made calls. You usually create one LCR table per site.

The following table is an example of an LCR table.

Country Code	Area Code	Prefix	Weighted Cost
1	408	565	0
1	408		0
1	650		0
1	415		5

The CMA system compares the dial string for a call to the dial strings in LCR tables. The dial string can match at the country code, area code, or prefix level. The CMA system reads the “# of digits to strip” field to determine how many digits to remove.



Note

For areas of the United States that do not require you dial an access code before the area code, exclude this number when you define the number of digits to strip.

Before determining the final call routing, the CMA system considers cost (through LCR tables), bandwidth resources (through site topology and device group policies), and gateway availability.

Example of Least-Cost Routing

Company ABC has three sites: Site A in San Jose, CA, Site B in Monterey, CA, and Site C in Washington, D.C. All sites have gateways.

LCR Tables for Three Sites

The LCR tables included area codes that are used frequently in each site and considered that calls are made frequently from Site C to Southern California.

The following table lists area codes for the San Francisco Bay Area and Southern California. The prefix 755 for the 408 area code applies for all numbers in Site A.

Area Code	Prefix	Weighted Cost
408	755	0
408		0
650		0
510		0
925		0
415		5
831		5
213		10
310		10
714		10
		20

The following table lists area codes for Washington, D.C., Eastern Maryland, and Northeastern Virginia.

Area Code	Prefix	Weighted Cost
202	238	0
202		0
240		0
301		0
741		0
703		0
410		5
443		5
540		5
804		10
		20

The following table lists area codes for San Jose, Monterrey, and Southern California.

Area Code	Prefix	Weighted Cost
831	477	0
831		0
408		5
213		10
310		10
714		10
		20

Call Scenario One

Site C can call San Jose using ISDN through one of two routes:

- Through the Site C gateway to the local phone system, making a long distance connection, at a higher cost per minute.
- From Site C through the direct inter-site link to Site A and out its gateway, at a lower cost per minute.



Note

If you dial an area code that is not in an LCR table, the call goes through the gateway from which the call originates.

Call Scenario Two

Calls are frequently made from Site C to Los Angeles. The area codes for some parts of Southern California are included in the LCR tables for Sites A and B, because it is less expensive to make an intrastate long distance call within California than an interstate long distance call from Washington, D.C. to Los Angeles.

By including Southern California area codes in LCR tables for San Jose and Monterey, if the bandwidth for the San Jose gateway is saturated, the call from Site C can be routed through the Monterey gateway. The priority is to call from Site A or Site B, because the LCR tables share a relative cost to dial the area codes for Los Angeles.

Determining Area Codes

It is recommended you enter area codes for:

- The area in which the site is located.
- The area surrounding the site.
- Frequently called numbers.

You should also include special rate plans for intrastate calling.

Determining Country Codes

If you make international calls and you determine that calls to a certain country are less expensive from a particular gateway, enter the dial string for this country in the LCR table for the selected gateway.

Determining the Weighted Cost

When you enter call strings in an LCR table, associate a weighted cost with each one. You can base the cost on a monetary value or ratio that compares costs between several locations. The weighted cost determines which call string is most cost-effective to use.

You can calculate costs for the following types of calls:

- Local
- Local toll
- Intrastate
- Interstate
- International long distance

Field	Description
Name	Name (ASCII only) for the LCR table.
Description	(Optional) (ASCII only)
Country	Country code for the location to which this call is made.
City Code	City or area code for the location to which this call is made.
Prefix	The prefix is the first three numbers in a 7-digit dial string.
# Digits to Strip	The number of digits to strip before dialing.
Cost	Weighted cost for each call to the selected area or city code.

LCR operations include:

- [View the Least Cost Routing Tables List](#)
- [Add a Least Cost Routing Table](#)
- [Edit a Least Cost Routing Table](#)
- [Delete a Least Cost Routing Table](#)

View the Least Cost Routing Tables List

Column	Description
Name	Name of the LCR table.
Description	Description of the LCR table.

To display the list of least cost routing tables

- Go to **Admin > Dial Plan > LCR Tables**.

The **LCR Tables** list appears.

Add a Least Cost Routing Table

To add a LCR table

- 1 Go to **Admin > Dial Plan > LCR Tables**.
- 2 In the **LCR Tables** list, click **Add LCR**.
- 3 In the **Add LCR Tables** dialog box, enter the **Name**, **Description**, and **New Route** information required to create a new table.
- 4 Click **Add**.
- 5 Repeat step 3 and 4 for add additional routes to the table.
- 6 Click **OK**.

Edit a Least Cost Routing Table

To edit an LCR table

- 1 Go to **Admin > Dial Plan > LCR Tables**.
- 2 In the **LCR Tables** list, select the table of interest and click **Edit LCR**.

- 3 In the **Edit LCR** dialog box, edit the **Name**, **Description**, and **New Route** information as required.

- 4 Click **Save**.

The changes you made apply to all MCUs associated with a gateway service that uses this LCR table.

Delete a Least Cost Routing Table

To delete an LCR table

- 1 Go to **Admin > Dial Plan > LCR Tables**.
- 2 In the **LCR Tables** list, select the table of interest and click **Delete LCR**.
- 3 Click **Delete** to confirm the deletion.

E.164 Numbering Scheme

E.164 Implementation in the CMA System

The Polycom E.164 implementation is based on an E.164 Telecommunications Recommendation and provides E.164 functionality within the Polycom CMA environment.

The CMA system provides the ability to automatically generate E.164 aliases through its E.164 numbering scheme feature. This feature effectively works as an E.164 alias generator and allows for two types of E.164 number generation: default or custom. When the CMA system is setup correctly, it will generate one E.164 alias per dynamically-managed endpoint.

E.164 Alias Assignment

The CMA system can assign an E.164 alias to each dynamically-managed endpoint at the time of first registration with the CMA System. An E.164 alias assignment will be based on the default E.164 numbering scheme or on a specified E.164 numbering scheme, if one has been setup. However, if an E.164 alias already exists in a Dial String Reservation for a User or Room, then it will have priority over the E.164 number generation.

E.164 aliases may also originate from other CMA system sources to include a User or Room Dial String Reservation, a Guest E.164 designation, and an E.164 alias provided directly at the endpoint (this option is only applicable to some non-dynamically-managed endpoints).

Within the CMA system, an E.164 alias provided in a Dial String Reservation has a higher priority than a generated E.164 alias.

A single user with multiple endpoints may be assigned a unique E.164 alias per endpoint.



IMPORTANT

H.323 must be enabled on an endpoint and the it must be registered with the Gatekeeper, prior to the CMA system's application of the E.164 numbering scheme.H.323 can be enabled on an endpoint through the CMA system's site provisioning functionality. See [“Add a Site”](#) on page 461.

E.164 Numbering Scheme Default Settings

The E.164 numbering scheme functionality consists of three main parts: prefix, base field, and suffix. The entire E.164 numeric string has a 15-digit maximum.

Prefix	Base Field	Suffix
Based on Device Type Choosing this selection will automatically associate a unique two-digit identifier to each dynamically-managed endpoint type. See the “Based on Device Type Settings” section.	Specify Number Range The number range has been preset to 1000 and 9999. Important When a numeric range runs out of numbers, the number generation operation will fail.	No Suffix A suffix will not be assigned to the Default E.164 Numbering Scheme (Alias).
The number below is only an example of a Prefix assignment.	The number below is only an example of a Base Field assignment.	The lack of a number below, is only an example of a No Suffix assignment.
44 (sample value)	1009 (sample value)	(blank sample value)

E.164 Numbering Scheme Explained

To give you an idea of how an E.164 numbering scheme would appear, see example below. Please note that the example is based on sample default values provided in the table above.

441009 (an example of an E.164 Alias)

Here the **Prefix** is derived from the **Based on Device Type** selection, in this case, the “44” in the sample is referring to a Polycom RealPresence Group Series endpoint, this number will normally adjust to match the actual endpoint type.

The “1009” assignment is a sample **Base Field** result derived from the **Number Range** selection, in this example, the range is between 1000 and 9999.

The **Suffix** portion of this example was set to **No Suffix**, which means that a suffix value will not be appended to the resulting E.164 Alias.

Field	Description
Prefix	<p>The Prefix is the first part of the E.164 Numbering Scheme and contains up to three options</p> <ul style="list-style-type: none"> • No Prefix • A Number (specify) • Based on Device Type, available only if shown <p>The first option, No Prefix, means that there will not be any digits listed in front of the Base Field assignment</p> <p>The second option, A Number, (specify) allows for the specification of up to 7 digits, be careful, not to go over the allowable 15-digit maximum.</p> <p>The third option, Based on Device Type, will only be visible in the Prefix if it has not been already selected in the Suffix.</p> <p>If the Based on Device Type selection is available for selection, it will use the two-digits predefined device type. See the Based on Device Type Settings section.</p>
Base Field	<p>There are two available options for the Base Field</p> <ul style="list-style-type: none"> • Specify Number Range... • Phone Number <p>The first option, Specify Number Range..., allows for the designation of a numeric range. The range may fall anywhere from 0 through 9999999999.</p> <p>The second option, Phone Number, allows for the assignment of a phone number from the Active Directory along with the number of digits to utilize from the phone number, and can range anywhere between 3 to 10 digits. Or, in the event a phone number does not exist, a numeric range will be used instead, if defined, and it can be anywhere from 0 through 9999999999</p>
Suffix	<p>The suffix is the last part of the three-part E.164 Numbering Scheme and may contain up to three of its own options.</p> <ul style="list-style-type: none"> • No Suffix • A Number (specify) • Based on Device Type. <p>The first option, No Suffix, means that there will not be any digits listed after the Base Field designation of the E.164 Alias.</p> <p>The second option, A Number (specify), allows for the specification of up to 7 digits, be careful not to exceed the allowable 15 digit minimum.</p> <p>The third option, Based on Device Type, will use the two-digits predefined device type. See the Based on Device Type Settings section.</p>

Based on Device Type Settings

The CMA system's **Based on device Type** option is mutually exclusive to the prefix or suffix portion of the E.164 numbering scheme functionality.

The CMA system will generate this type of prefix or Suffix by matching the actual endpoint type to the predefined CMA system values listed below.

RealPresence Group Series -----	44
CMA Desktop -----	22
RealPresence Desktop -----	66
VVX -----	33
RealPresence Mobile -----	55
HDX -----	11

Generating E.164 Aliases

An Administrator may choose to use the default E.164 number generation scheme or create a distinct E.164 numbering scheme that is better suited to their existing IT environment.

To use the E.164 number generation scheme, ensure that H.323 functionality is enabled on the endpoints. H.323 can be enabled on the endpoints via site provisioning through the CMA system. For more information about site provisioning, see [“Add a Site”](#) on page 461.

To customize an E.164 number generation scheme

- 1 Go to **Admin > Dial Plan and Sites > E.164 Numbering Scheme**
- 2 In the **Prefix** section, select your option. The available options are: **No Prefix**, **A Number (specify)**, **Based on Device Type** (if available for selection).
- 3 In the **Base Field** section, select your preferred option. The available options are: **Specify Number Range** and **Phone Number**.
- 4 In the **Suffix** section, select your preferred option. The available options are: **No Suffix**, **A Number (specify)**, **Based on Device Type** (if available for selection).
- 5 Click **Update**.

Setting-up an E.164 Alias in a User Dial String Reservation

To setup an E.164 alias for an existing user

- 1 Go to **User > Users**
- 2 Highlight a specific user.

- 3 Click on **Edit**. The **Edit User** dialog will display.
- 4 Click on **Dial String Reservations**.
- 5 Select your endpoint type.
- 6 In the **E164** field, enter an **E.164 Alias**.
- 7 Click **Apply** then **Update**.

- 1 Go to **User > Users**
- 2 Click on **Add**. The **Add User** dialog will display.
- 3 Click on **Dial String Reservations**.
- 4 Select your endpoint type.
- 5 In the **E164** field, type in an **E.164 Alias**.
- 6 Click **Apply** then **Update**.

Setting-up an E.164 Alias in a Room Dial String Reservation

To setup an E.164 alias for an existing room

- 1 Go to **Admin > Rooms**
- 2 Highlight a specific room.
- 3 Click on **Edit**. The **Edit Room** dialog will display.
- 4 Click on **Dial String Reservations**.
- 5 Select your endpoint type.
- 6 In the **E164** field, type in an **E.164 Alias**.
- 7 Click **Apply** then **Update**.

To setup an E.164 alias for a new room

- 1 Go to **Admin > Rooms**
- 2 Click on **Add**. The **Add New Room** dialog will display.
- 3 Click on **Dial String Reservations**.
- 4 Select your endpoint type.
- 5 In the **E164** field, type in an **E.164 Alias**.
- 6 Click **Apply** then **Update**.



Note

The total number of digits specified for an E.164 numbering scheme (alias) must be 15 digits or less. If a user's phone number is assigned to the Base Field, the system reserves one digit to differentiate between the user's multiple devices. In this case, the total number of digit cannot exceed 14 digits

The E.164 number generation is only applicable to dynamically-managed endpoints.

Remote Alert Setup Operations

This chapter describes how to configure the Polycom® Converged Management Application™ (CMA®) system to send alerts to users via E-mail for specific types of system and endpoint events. It includes these topics:

- [Set Up Remote Alerts](#)
- [Edit a Remote Alert Profile](#)
- [Disable a Remote Alert Profile](#)
- [Delete a Remote Alert Profile](#)
- [Disable CMA System Remote Alerts](#)

Set Up Remote Alerts

The CMA system remote alerts functionality is very flexible. It allows you to:

- Assign different severity levels to different classifications of CMA system and Endpoint alerts.
- Create different alert profiles so that different types of alerts can be sent to different people. So if you have administrators who specialize by device type (for example bridges, endpoints, or servers), you can create profiles that notify each type of administrator of failures related to those specific types of devices.

To set up remote alerts, you must complete the following tasks:

- 1 [Set Up CMA System-generated E-mail Account.](#)
- 2 [Enable CMA System Remote Alerts.](#)
- 3 [Set CMA System Remote Alert Level Settings.](#)
- 4 [Set Endpoint Alert Level Settings.](#)
- 5 [Add a Remote Alert Profile.](#)
- 6 [Associate a Remote Alert Profile With a User.](#)

Set Up CMA System-generated E-mail Account

To set the CMA system-generated E-mail account

- 1 Go to **Admin > Server Settings > E-mail**.
- 2 On the **E-mail** page, enter the E-mail account (ASCII only) from which the CMA system will send conference notification E-mails and system alerts.

By default, the CMA system E-mails are sent from the *PanAlert@vtcmanager.com* E-mail account.
- 3 Specify the IP address of the mail server from which the CMA system will send conference notification E-mails.



Notes

- Many E-mail servers will block or discard E-mails without a qualified From: address. To avoid this issue, make sure each person with Scheduler permissions has a valid E-mail address.
- Many E-mail servers will block or discard E-mails from untrusted domains, in which case you may need to change the default CMA system E-mail address to one in a trusted domain.

- 4 Click **Update**.

Enable CMA System Remote Alerts

To enable Polycom CMA system remote alerts

- 1 Go to **Admin > Server Settings > Remote Alert Setup**.
- 2 On the **Remote Alert Setup** page, select **Enable Remote Alerts**.
- 3 Set a **Remote Alert quiescent time**, which is the amount of time (in minutes) the system should wait after alerts have been detected but not cleared before starting the alert notification process, and if applicable, the remote alert notification process.
- 4 Click **Update**.

Set CMA System Remote Alert Level Settings

The CMA system monitors and reports events regarding its performance, connections, and services. It categorizes alerts into three alert levels: **Info**, **Minor**, or **Major**.

By default the **Alert Severity Level** is set to **Info** for all of the **CMA Alert Types** it reports. You have these options:

- You can leave all of the **Alert Severity Levels** set to **Info** and create a single remote alert profile that allows you to notify all users assigned that profile about system events of all types.
- You can change some of the **Alert Severity Levels** to either **Minor** or **Major** and create multiple remote alert profiles that notify different users of system events of different types and severity levels.

To set the CMA system remote alert level settings

- 1 Go to **Admin > Alert Settings > CMA Alert Level Settings**.
- 2 On the **CMA Alert Level Settings** page, change the **Alert Severity Level** for the following **CMA Alert Type** system events, as required.

Alert Type	Alert indicates...
Bridge Down	A Polycom MCU (RMX or MGC) has failed.
Database Connection Down	The connection to the database has been lost.
Enterprise Directory Connection Down	The connection to the enterprise directory server has been lost.
Enterprise Directory System Account Password Failure	The connection to the enterprise directory server could not be established because the account password was incorrect.
CMA Failover Occurred	(In redundant CMA system configurations only.) The system has failed over from one system server to the other.
License Capacity Threshold Exceeded	The number of available seats defined by the installed license is within 5% of the total license capacity.
Bridge Time Discrepancy	A difference between the clock on the Polycom MCU (RMX or MGC) and the CMA system clock.
CMA Monitor Service Stopped	(In redundant CMA system configurations only.) The CMA system redundancy monitoring service is not running.

Alert Type	Alert indicates...
Redundant Server Down	(In redundant CMA system configurations only.) The connection or synchronization between the primary and secondary server has been lost.
Redundancy Conflict	(In redundant CMA system configurations only.) Both the primary and secondary system servers believe they are the active server.
Site Bandwidth Threshold Exceeded	The site bandwidth threshold, which is set at 90% of capacity, has been exceeded.
Subnet Bandwidth Threshold Exceeded	The subnet bandwidth threshold, which is set at 90% of capacity, has been exceeded.
Site Link Bandwidth Threshold Exceeded	The site link bandwidth threshold, which is set at 90% of capacity, has been exceeded.
Active Call Exceeded 90% of Maximum	<p>The number of active calls has exceeded 90% of the maximum allowed. This value is dependent on the call model (routed or direct) and the total number of licenses.</p> <ul style="list-style-type: none"> In routed mode, the maximum number of active calls is 30% of the total number of licenses. In direct mode, the maximum number of active calls is 60% of the total number of licenses.
Active Call Exceeded 100% of Maximum	<p>The number of active calls has exceeded 100% of the maximum allowed. This value is dependent on the call model (routed or direct) and the total number of licenses.</p> <ul style="list-style-type: none"> In routed mode, the maximum number of active calls is 30% of the total number of licenses. In direct mode, the maximum number of active calls is 60% of the total number of licenses.
E164 Alias Assignment Failed	The CMA system was unable to assign an E.164 alias to the endpoint.
Certificate Expiration Warning	The specified certificate will expire in 30 days. If the certificate is not renewed within 30 days, the alert continues daily.
Certificate Expired Warning	The specified certificate has expired. The alert continues daily until the certificate is renewed or removed.
Database Backup Failure	The database backup has failed.
Used disk space reaches ____% of the total disk space	Disk space threshold, as entered in the text box, has been exceeded.

3 Click **Update**.

Set Endpoint Alert Level Settings

Monitored endpoints send events to the CMA system. The CMA system categorizes and reports endpoint alerts into three alert levels: **Info**, **Minor**, or **Major**.

By default the **Alert Severity Level** is set to **Info** for all of the **Endpoint Alert Types** it reports. You have these options:

- You can leave all of the **Alert Severity Levels** set to **Info** and create a remote alert profile for each endpoint type being monitored that allows you to notify all users assigned that profile about all endpoint events applicable to that endpoint type.
- You can change some of the **Alert Severity Levels** to either **Minor** or **Major** and create multiple remote alert profiles that notify different users of endpoint events of different types and severity levels.

To set the endpoint alert level settings

- 1 Go to **Admin > Alert Settings > Endpoint Alert Level Settings**.
- 2 On the **Endpoint Alert Level Settings** page, change the **Alert Severity Level** for the different types of endpoint events as required.

Alert Type	Alert indicates...
Remote Control Battery Low	The battery in the endpoint's remote needs to be replaced.
Credentials Required	The endpoint system requires that the user enter a valid username and password.
Credentials Failed	An attempt to log into the endpoint system failed.
HTTP Forbidden	The endpoint must be used in <i>https:</i> mode only.
Device Not Responding	The endpoint is not responding to the CMA system.
Heartbeat Timeout	The endpoint did not send a heartbeat to the CMA system within the required timeout period.
Gatekeeper Status Unknown	The CMA system gatekeeper cannot determine the connection status of the endpoint.
Gatekeeper Rejected	The CMA system gatekeeper rejected the endpoint's attempt to register.
Gatekeeper Unregistered	The endpoint is not registered to the gatekeeper.

Alert Type	Alert indicates...
Directory Status Unknown	The CMA system gatekeeper cannot determine the directory status of the endpoint.
Directory Not Registered	The endpoint is not registered to the directory service.
Presence Status Unknown	The CMA system gatekeeper cannot determine the presence status of the endpoint.
Presence Unregistered	The endpoint is not registered to the presence service.
User Assistance Request	The endpoint user sent a request for help.
Management URL Not Set	<p>The CMA system is not one of the management URLs set on the endpoint, possibly because the management URL list is full.</p> <p>Note</p> <p>Because endpoint systems do not have an interface to manually delete management URLs, if the management list is full you must disconnect the endpoint's network cable for two minutes. This should clear up all the mgmt server URLs.</p>
Touch Control Disconnected	The Touch Control device that was connected to the listed HDX is no longer connected to the HDX.
Touch Control Software Incompatible with Endpoint	The software version of the Touch Control platform is not compatible with the Endpoint software version.
SIP URI Not Provisioned	A dynamically-managed endpoint at a site with SIP enabled does not have a SIP dial string reservation. The endpoint is provisioned without SIP enabled.
SIP Status Unknown	The SIP server cannot determine the status of the endpoint.
SIP Unregistered	The endpoint is not registered with the SIP server.

3 Click **Update**.

Add a Remote Alert Profile

You can add a remote alert profile to identify which device alerts from which devices should be sent as part of a remote alert profile. Note that using a combination of setting alerts by device type and by specific types, provide additional granularity in managing device alerts.

To add a remote alert profile

- 1** Go to **Admin > Alert Settings > Remote Alert Profiles**.
- 2** On the **Remote Alert Profiles** page, click **Add**.
- 3** In the **Add Remote Alert Profile** dialog box, enter a **Name** and **Description** for the profile.
- 4** To activate the profile, select **Enable Profile**.
- 5** Configure one of the following:
 - To have all CMA system alerts sent as part of this profile, select **Info, Minor, and Major**.
 - To have a subset of CMA system alerts sent as part of this profile, select any combination of **Info, Minor, or Major**. These selections work in conjunction with the CMA system alert level settings you chose previously.
 - To have no CMA system alerts sent as part of this profile, leave **Info, Minor, and Major** cleared.
- 6** To use the device type to identify which devices and device alerts should be sent as part of this profile, click **Alert by Device Type** and configure one of the following. For endpoint systems, these selections work in conjunction with the endpoint alert level settings you choose previously.
 - a** To have all device alerts for all device types sent as part of this profile, in the **Device Type Alert Level Mapping** page, select **Info, Minor, and Major** for all of the device types.
 - b** To have a subset of device alerts for all device types sent as part of this profile, in the **Device Type Alert Level Mapping** page, select any combination of **Info, Minor, or Major** for each device type.
 - c** To have all device alerts for a subset of device types sent as part of this profile, in the **Device Type Alert Level Mapping** page, select **Info, Minor, or Major** for each device type to be included in the profile. Alerts for those device types that do not have an alert level selected will not be included.
- 7** To use the device name to identify which devices and device alerts should be sent as part of this profile, click **Alert by Device**.

**Notes**

- If you set device alerts for specific devices, these settings override settings made on the **Alert by Device Type** page. The settings are not cumulative.
- You cannot set the system up to send device alerts for specific desktop video endpoints. Polycom CMA Desktop and Polycom PVX endpoints are not displayed in the **Available Device** list.

- a** As needed, use the **Filter** to customize the device list.

- b** In the **Available Devices** list, select the devices to add to the profile. Use **CTRL** to select multiple devices.
 - c** Click the down arrow to add the devices to the **Monitored Devices** list and configure one of the following:
 - » To have all device alerts for all selected devices sent as part of this profile, for the devices in the **Monitored Devices** list, select **Info**, **Minor**, and **Major** for each device.
 - » To have a subset of device alerts for all selected devices sent as part of this profile, for the devices in the **Monitored Devices** list, select any combination of **Info**, **Minor**, or **Major** for each device.
 - » To have all device alerts for a subset of device types sent as part of this profile, for the devices in the **Monitored Devices** list, select **Info**, **Minor**, and **Major** for each device to be included in the profile. Alerts for those devices in the **Monitored Devices** list that do not have an alert level selected will not be included.
- 8** Click **OK**.

Associate a Remote Alert Profile With a User

To associate a remote alert profile with a user

- 1** Go to **User > Users**.
- 2** To search for a user:
 - a** In the **Search** field of the **Users** page, search for the user of interest.



Note

Searches for a user on the CMA system **Users** page are case-insensitive, prefix searches of the **Username**, **First Name**, and **Last Name** fields.

- b** To search both local and enterprise users, clear the **Local Users Only** check box and press **Enter**.
The first 500 users in the database that match your search criteria are displayed in the **Users** list.
 - c** If the list is too large to scan, further refine your search string.
- 3** Select the user of interest and click **Edit User**.
 - 4** In the **Edit User** dialog box, click **Associated Alert Profile**.
 - 5** Select the **Remote Alert Profile** to associate with the user.
 - 6** Click **OK**.

Edit a Remote Alert Profile

To edit a Remote Alert Profile

- 1 Go to **Admin > Alert Settings > Remote Alert Profiles**.
- 2 On the **Remote Alert Profiles** page, select the profile of interest and click **Edit Remote Alert Profile**.
- 3 As required, edit the **General Info**, **Alert by Device Type**, and **Alert by Device** sections of the **Edit Remote Alert Profile** dialog box.
- 4 Click **OK**.

Disable a Remote Alert Profile

To disable a Remote Alert Profile

- 1 Go to **Admin > Alert Settings > Remote Alert Profiles**.
- 2 On the **Remote Alert Profiles** page, select the profile of interest and click **Edit Remote Alert Profile**.
- 3 Clear **Enable Profile**.
- 4 Click **Update**.

Delete a Remote Alert Profile

To delete a Remote Alert Profile

- 1 Go to **Admin > Alert Settings > Remote Alert Profiles**.
- 2 On the **Remote Alert Profiles** page, select the profile of interest and click **Delete Remote Alert Profile**.
- 3 Click **Yes** to confirm the deletion.

The profile is deleted from the CMA system.

Disable CMA System Remote Alerts

To disable all (system and device) CMA System remote alerts

- 1** Go to **Admin > System Settings > Remote Alert Setup**.
- 2** On the **Remote Alert Setup** page, clear **Enable Remote Alerts**.
- 3** Click **Update**.

System Management and Maintenance

This chapter describes the following Polycom® Converged Management Application™ (CMA®) system operations topics:

- [Management and Maintenance Overview](#)
- [Recommended Regular Maintenance](#)

Management and Maintenance Overview

The CMA system requires relatively little ongoing maintenance beyond monitoring the status of the system and downloading backups you want to archive. All system management and maintenance tasks can be performed in the management interface. See the appropriate topic for your user role:

- [Administrator Responsibilities](#)
- [Auditor Responsibilities](#)

Administrator Responsibilities

As a CMA system administrator, you're responsible for the installation, configuration, and ongoing maintenance of the system. You should be familiar with the following tasks and operations:

- Installing licenses when the system is first installed and when additional endpoints are added. See [“Polycom CMA System Licensing”](#) on page 384.
- Monitoring system health and performing the recommended regular maintenance. See [“Recommended Regular Maintenance”](#) on page 523.
- Using the system tools provided to aid with system and network diagnostics, monitoring, and troubleshooting. See [“System Troubleshooting”](#) on page 529. Should the need arise, Polycom Global Services personnel may ask you to use these tools.

- Upgrading the system when upgrades/patches are made available. See [“Update the Polycom CMA System Software”](#) on page 445.

Administrative Best Practices

The following are some of our recommendations for administrative best practices:

- Perform the recommended regular maintenance.
- Except in emergencies or when instructed to by Polycom Global Services personnel, don't reconfigure, install an upgrade, or restore a backup when there are active conferences on the system. Many of these operations will require a system restart to complete, which will result in conferences being dropped.
- Before you reconfigure, install an upgrade, or restore a backup, manually create a new backup of the system settings. Then download and archive this backup in the event that something unforeseen occurs and it becomes necessary to restore the system to a known good state.
- For proper name resolution and smooth network operations, configure at least one DNS server in your network configuration, and preferably two or more. This allows the CMA system to function properly in the event of a single external DNS failure.
- Configure at least one NTP server in your time configuration and preferably two or more. Proper time management helps ensure that your cluster operates efficiently and helps in diagnosing any issues that may arise in the future. Proper system time is also essential for accurate audit and CDR data.

Auditor Responsibilities

As a CMA system auditor, you're responsible for managing the system's logging and history retention. You should be familiar with the following configurations and operations:

- Configuring logging for the system. These settings affect the number and the contents of the log archives available for download from the system. Polycom Global Services personnel may ask you to adjust the logging configuration and/or download and send them logs.
- Configuring history retention levels for the system. These settings affect how much system activity history is retained on the system and available for download as CDRs.

Auditor Best Practices

The following are some of our recommendations for auditing best practices:

- Unless otherwise instructed by Polycom Global Services, configure logging at the production level with a rolling frequency of every day and a retention period of 60 days. If hard drive space becomes an issue, decrease the retention period incrementally until the disk space issue is resolved.
- Download log archives regularly and back them up securely (preferably offsite as well as onsite).
- Export CDRs regularly and back them up securely (preferably offsite as well as onsite).

Recommended Regular Maintenance

Perform the following tasks to keep your CMA system operating trouble-free and at peak efficiency. These tasks can be done quickly and should be run at least weekly.

Create and Archive Backups

Log into the CMA system, go to **Admin > Backup System Settings and Create and Download a Backup Archive**. For more information, see [“Backup the CMA System Settings”](#) on page 526.

General System Health and Capacity Checks

On the **Dashboard** verify that there are no alerts indicating problems with any part of the system. For more information, see [“Polycom CMA System Dashboard”](#) on page 307.

Certificates

Go to **Admin > Management and Security > Certificate Management** and verify that the list of certificates contains the certificates you’ve installed and looks as you would expect (an archived screen capture may be helpful for comparison).

Display the details for any certificate you’ve installed and verify they are as expected (an archived screen capture may be helpful for comparison). For more information, see [“Manage Certificates”](#) on page 446.

CDR export

If you want to preserve detailed call and conference history data in spreadsheet form off the Polycom CMA system, periodically download the system’s CDR (call detail record) data to your PC.

System Backup and Recovery Operations

This chapter provides an overview of the Polycom® Converged Management Application™ (CMA®) backup and recovery procedures.

The backup and recovery of a CMA system includes backup and recovery of the CMA system internal database and the backup of the CMA system configuration settings. It includes these topics:

- [Backup Internal Databases and System Configuration](#)
 - [Backup the CMA System Internal Databases](#)
 - [Backup the CMA System Settings](#)
- [Restore Database and System Configuration](#)
 - [Restore to Factory Default Image](#)
 - [Restore from a Backup Archive](#)

Backup Internal Databases and System Configuration

Users assigned the **Administrator** role have two backup options. They can:

- Generate backups of just the internal CMA database files (*.bak* format)
OR
- Create and download a system backup archive (*.zip* format), which includes both the internal database backup files and the system settings.

We recommend creating and downloading a system archive weekly. This archive makes system restoration much simpler.

Backup the CMA System Internal Databases

This topic describes how to create a backup of the CMA system internal database files. These database backup files cannot be used to restore the internal databases to a CMA system. These files can be used for troubleshooting or to migrate the system to an external database system.

To backup the CMA system internal databases only

- 1 From the CMA system web interface, go to **Admin > Backup System Settings**.
- 2 When the **Backup System Settings** page appears, click **Generate Database Backup Files**.

A dialog box appears indicating that the database backup has been initiated and the operation will take some time.

- 3 To view the list of backup files including those generated in step 2, go to **Admin > Database Backup Files**.

The **Database Backup Files** list appears showing all of the backup files stored on the CMA system. Files with a timestamp included in the name are system-generated backup files. Files without a timestamp are user forced backups.

- 4 To save the downloaded backup files only, select the backup files of interest and click **Save**.
- 5 In the **File Download** dialog box, click **Save**, browse to a location on your system, and click **Save**.

Backup the CMA System Settings

This topic describes how to create a backup archive of a CMA system, including system configuration settings and internal database files. Once the backup archive is downloaded, it can be used to restore the system to its last archived configuration after a disastrous system failure.

To backup the CMA system settings

- 1 From the CMA system web interface, go to **Admin > Backup System Settings**.
- 2 When the **Backup System Settings** page appears, click **Create and Download a Backup Archive**.
- 3 In the **Select location for download** dialog box, enter a unique **File name**, browse to a location on your system and click **Save**.

A **File Download** dialog box displays the progress of the download operation.

- 4 When the operation is completed, click **OK**.
- 5 Browse to the location specified in step 3 and verify the file download.

Restore Database and System Configuration

A user assigned the **Administrator** role can restore a CMA system using a backup archive. To restore an CMA system, follow the procedures in this topic.

To restore a system from a backup archive

- 1 [“Restore to Factory Default Image”](#) on page 527.
- 2 **Perform First Time Setup**. For more information about First Time Setup, see the *Polycom CMA System Getting Started Guide* for this release.
- 3 [“Restore from a Backup Archive”](#) on page 528 using the last archived configuration. The archived configuration will overwrite the configuration that resulted from **First Time Setup**. The only CMA system configuration settings not included in the archive and thus not overwritten are the network settings and the security certificates required for an operational system.

In cases when the CMA system is functional, but the configuration or database is corrupted, the backup archive can also be used to return a CMA system back to its last known good archive. As long as the network settings and security certificates are operational, the last known good archive will return the CMA system to its former functional state.

Restore to Factory Default Image

In a disaster recovery situation, your Polycom Global Services (PGS) support representative may be required to restore your CMA system to its factory default image.

To perform this disaster recovery procedure, you will need the **Restore to Factory Default DVD** that shipped with the CMA system server. This DVD has the base image of the CMA system server software.




WARNING

- This is a last resort, so never do this without being instructed to do so by PGS support.
- This process will wipe out your system database and all other system data.
- The **Restore to Factory Default DVD** is specific to the CMA system server type and version.

Restore from a Backup Archive

A user with the **Administrator** role can restore the CMA system using a backup archive.

To restore a backup archive

- 1 Go to **Admin > Backup System Settings**.
- 2 In the **Select Archive File** section of the **Backup System Settings** page, click .
- 3 In the **Select file to upload** dialog box, select the archive file to upload and click **Open**.
- 4 Click **Restore from Backup Archive**.

Two warnings appear about the backup process. The second warns that the process is irrevocable and may result in an usable system.

- 5 Click **OK**.

The system uses the archive file to restore the CMA system to the state of the backup files.

When the CMA system is functional, but the configuration or database is corrupted, [“Restore from a Backup Archive”](#) on page 528 can also return a CMA system to its last known good archive. As long as the network settings and security certificates are operational, the last known good archive will return the CMA system to its former functional state.

System Troubleshooting

This chapter provides Polycom® Converged Management Application™ (CMA®) system troubleshooting information. It includes the following topics:

- [Troubleshooting Utilities Dashboard](#)
- [Troubleshooting Specific Types of Issues](#)
 - [Registration Problems and Solutions](#)
 - [Point-to-Point Calling Problems and Solutions](#)
 - [MCU and Gateway Dialing Problems and Solutions](#)
 - [Conference On Demand Problems and Solutions](#)

Troubleshooting Utilities Dashboard

The CMA system has a **Troubleshooting Utilities** dashboard that brings together on one page access to all of the information you might need to diagnose system issues. It includes access to various diagnostic files and informational panes.

The diagnostic files include:

- **Traces** – Use this option to generate and download a network sniffer trace that can help you examine the traffic to and from the CMA system.
- **Windows Event Logs** – Use this option to generate and download a *WindowsEventLogs.zip* file that includes the **Application**, **Security**, and **System** logs. These logs store events logged by applications, events related to logon and resource use, and events logged by Windows system components respectively. For more information about these event logs, see [Microsoft Technet](#).
- **CMA System Logs** – Use this option to generate and download a *GetAllLogs.zip* file that includes all of the CMA system log files. For more information about these system logs, see [“View and Export System Log Files”](#) on page 300.

- **CMA System Report** – Use this option to generate and download a *SystemInfo.txt* file that describes the system configuration. For more information about this report, see [“CMA System Report”](#) on page 303.
- **Database Backup** – Use this option to initiate a backup of selected CMA internal databases.
- **Test Network Connection** – Use this option to perform a **Traceroute** or **Ping** operation. **Traceroute** allows you to investigate the route path and transit times of packets as they travel across an IP network. **Ping** allows you to test the availability of a host on an IP network..
- **Synchronize Certificate Stores** – Use this option to reset all certificate stores with the currently uploaded certificates and certificate revocation lists (CRLs).

The information panes include:

- **Systems** – Displays summary information about the devices registered with the CMA system. For more information, see [“Systems”](#) on page 315.
- **CMA Configuration** – Displays information about the configuration of the CMA system. For more information, see [“CMA Configuration”](#) on page 309.
- **CMA Info** – Displays general information about the CMA system. For more information, see [“CMA Info”](#) on page 310.
- **CMA Licenses** – Displays information about how the CMA system is licensed. For more information, see [“CMA Licenses”](#) on page 313.
- **Gatekeepers** – Displays information about the CMA system as a gatekeeper. For more information, see [“Gatekeepers”](#) on page 312.
- **Users Logged In** – Displays the type and number of users that are currently logged into the system. For more information, see [“Users Logged In”](#) on page 309.
- **Services** – Displays information about the CMA system services. For more information, see [“Services”](#) on page 311.

Troubleshooting Specific Types of Issues

This section describes information on troubleshooting specific types of issues on the CMA system. It includes these topics:

- [Registration Problems and Solutions](#)
- [Point-to-Point Calling Problems and Solutions](#)
- [MCU and Gateway Dialing Problems and Solutions](#)
- [Conference On Demand Problems and Solutions](#)

Registration Problems and Solutions

Problem	Description	Solutions
Unable to place calls to an MCU conference room from a registered Polycom HDX system	The CMA system rejects the ARQ stating that the "endpoint is not registered" to the gatekeeper even though the system indicates it is registered.	<ul style="list-style-type: none"> • The MCU is not registered to the gatekeeper
When the gatekeeper registration is set to auto-discovery, endpoints do not register.	When auto-discovery is used, a GRQ message is broadcast and sent over multicast. However, the CMA system must be able to receive one of these messages, and does not respond to this message if it is not the default gatekeeper.	<ul style="list-style-type: none"> • Verify that the Default Gatekeeper check box is selected in the Admin > Gatekeeper Settings > Primary Gatekeeper page. • Verify that a UDP broadcast from the endpoint's network can reach the CMA system, or that multicast is enabled on all routers between the endpoint and the CMA system.
An endpoint cannot register with the CMA system.	<p>The endpoint is configured to use the CMA system as its gatekeeper, but is being rejected during registration.</p> <p>In the gatekeeper diagnostic log, an error has occurred during the RRQ/RCF process that caused the registration to fail.</p>	<ul style="list-style-type: none"> • Review the gatekeeper diagnostic logs for the RRQ attempt by the endpoint and determine the RRJ reason. • Verify that the endpoint alias is not a duplicate of other endpoint aliases. • Verify that the endpoint does not have NAT enabled. • Verify that enough licenses remain.
An endpoint cannot register with the CMA system.	<p>An endpoint cannot register with CMA, but the gatekeeper diagnostics do not indicate a problem.</p> <p>The gatekeeper sent the RCF message, but the endpoint did not receive it.</p>	<ul style="list-style-type: none"> • Verify that the IP address that the gatekeeper sent to the endpoint is correct.

Problem	Description	Solutions
The MCU cannot register with the CMA system.	Some MCU vendors register with a GRQ message instead of an RRQ message. Some MCU vendors do not retry registration after a first attempt has failed.	<ul style="list-style-type: none"> Verify that the Default Gatekeeper check box is selected in the Admin > Gatekeeper Settings > Primary Gatekeeper page. Reset the MCU or MGC card to force registration to occur.
An endpoint shows that it is not registered to the gatekeeper in the Gatekeeper Registration field in the Device Status .	The CMA system receives the RRQ message, but not the LWRRQ message from the endpoint. The endpoint did not send a LWRRQ message within the offline timeout period specified in the Admin > Gatekeeper Settings > Primary Gatekeeper page.	<ul style="list-style-type: none"> Reboot the endpoint.
The RadVision OnLAN MCU continually changes state: from online to offline and offline to online.	The Radvision OnLAN MCU ignores the RCF Time to Live (TTL) field, which is filled in with the value that the administrator specified in the offline timeout field in the Admin > Gatekeeper Settings > Primary Gatekeeper page.	<ul style="list-style-type: none"> Reconfigure the Radvision OnLAN MCU to send the registration requests in the same time period specified in CMA. Add the MCU manually. Reboot the MCU to force registration to occur.
Some endpoints are not assigned ISDN numbers.	A registered H.323-only system was not assigned an ISDN number. The system could belong to a network that does not have ISDN number ranges assigned to it. No ISDN numbers are available to assign.	<ul style="list-style-type: none"> Verify that the endpoint belongs to the site that has assigned ISDN number ranges. To do so, go to Admin > Dial Plan and Sites > Sites and make sure the site has the correct ISDN range specified in the ISDN Number Assignment pane. Verify that ISDN numbers are available to assign. Verify that the RCF message "Can't find ISDN free pool" from the gatekeeper returns to the endpoint.
Endpoints that were previously registered and auto-assigned ISDN numbers are being rejected when attempting to register.	Inconsistent configuration in ISDN number assignment has occurred.	<ul style="list-style-type: none"> Verify that the previous ISDN range was changed.
When the CMA system is restarted, some registrants that were previously online are now offline.	Some endpoints do not reregister when the CMA system goes down. Some MCUs do not reregister automatically after two retries.	<ul style="list-style-type: none"> Reboot the MCU.

Point-to-Point Calling Problems and Solutions

Problem	Description	Solutions
ViewStation and ViaVideo have an incorrect RAS IP address.	These endpoints are configured with a NAT address and may not receive the RCF message from the gatekeeper.	The endpoints need to be reconfigured to disable NAT.
A call with an alias as the dial string from a registered endpoint cannot be placed to another registered endpoint. The two endpoints are in different sites.	<ul style="list-style-type: none"> The site link between the sites in which the endpoints reside is not correctly defined or is missing. No bandwidth is available to the site link. The calling bit rate is higher than the bit rate defined in the site link. ISDN alternate routing is not available. Dialing rules may not be enabled or may be set to block instead of route. 	<ul style="list-style-type: none"> Go to Admin > Dial Plan and Sites > Site Links and make sure that a site link exists between the two networks. Make sure that the IP addresses of both endpoints are included in their respective sites. If site topology is defined for both endpoints, verify that there is enough bandwidth in the site links between the two sites. Verify that the dialing bit rate is lower or equal to that of the maximum bit rate defined for the site links. If the endpoint is ISDN capable, verify that the ISDN parameter is correct.
Dialing by IP address fails.	<p>A registered endpoint cannot call an unregistered endpoint by IP address within the same site.</p> <p>A dialing rule is not enabled or is set to block instead of route.</p>	<ul style="list-style-type: none"> Check the Reports > Gatekeeper Message Log for error messages. Verify that the registered endpoint is registered. Verify that the Deny calls to/from unregistered endpoints check box is cleared. Go to Admin > Gatekeeper Settings > Primary Gatekeeper to change this setting. Verify that the IP address dialing rule is enabled and set to route.

MCU and Gateway Dialing Problems and Solutions

Problem	Description	Solutions
<p>Call fails when using an MCU service.</p> <p>Dialing an MCU service results in a network error.</p>	<p>The call using the MCU service is rejected because of one of the following:</p> <ul style="list-style-type: none"> • The MCU is not registered. • The MCU is offline. • The MCU prefix is not registered as an E.164 alias. • The MCU resource issue was sent through resource allocation indication or resource allocation. • The dialing rule is not enabled. • The priority of the dialing rule may be too high. • Services are not enabled. 	<ul style="list-style-type: none"> • Check the Reports > Gatekeeper Message Log for error messages indicating why the call failed. • Verify that the MCU is registered. • Verify that the MCU is online. If the device is offline, reboot it. • Verify that the MCU service is available. Go to the Admin > Dial Plan and Sites > Services page. Verify that the MCU service prefix is enabled and listed.
<p>Simplified dialing does not work.</p> <p>When you dial 9, you receive a network error.</p>	<p>The call using the simplified dialing service is rejected because of one of the following:</p> <ul style="list-style-type: none"> • The simplified dialing prefix service in the system configuration is disabled. • No gateway services are available. • There is insufficient BRI/PRI bandwidth. • The call uses a higher bit rate than the device policy group allows. 	<ul style="list-style-type: none"> • Check the Reports > Gatekeeper Message Log for error messages. • Verify that the gateway and simplified dialing service prefix is enabled. Go to Admin > Dial Plan and Sites > Services. • Verify that the gateway is registered.

Conference On Demand Problems and Solutions

Problem	Description	Solutions
<p>Dialing a Conference On Demand fails.</p> <p>Inviting other endpoints into a conference using the CON service fails.</p>	<p>The endpoint dials a CON service, and the call is rejected because of one of the following:</p> <ul style="list-style-type: none"> • The MCU is not registered or is offline. • The CMA system cannot log into the MGC. • The MGC has no resource available for the call. • The MGC's IP address is not entered in the CMA system. 	<ul style="list-style-type: none"> • Check the diagnostics log for an ARJ reason from this endpoint. • Verify that the MCU is registered with the CMA system and is online. • Verify that the MCU registered with the CMA system has the MCU's IP address filled out in the Devices list. • Verify that the MCU login ID and password for the CON service are correct. • Verify that the H.323 network service that the MCU is using is set as the default service. • Verify that the MCU has enough available resources to start this conference. • Verify that the CON service is enabled. Go to Admin > Dial Plan and Sites > Services.

Gatekeeper Cause Codes

Cause Code	Description
150	The gatekeeper is out of resources
151	The gatekeeper has insufficient resources
152	The gatekeeper registration version is invalid
153	The call signal address is invalid
154	The registering device's address is invalid
155	The registering device's terminal type is invalid
156	The registering device's permissions are invalid
157	The conference ID is invalid
158	The registering device's ID is invalid
159	The caller's device is not registered
160	The called party's device is not registered

Cause Code	Description
161	The registering device's permissions have expired
162	The registering device has a duplicate alias
163	The call transport is not supported
164	The called device has a call in progress
165	The call has been routed to the gatekeeper
166	Cannot request a drop for others
167	The registering device is not registered with the gatekeeper
168	Unknown reason
169	Permission failure
170	Discovery permissions have expired
171	The device is not registered
172	No bandwidth available
173	Location not found
174	Security access denied
175	Quality of service not supported
176	Resources are exhausted
177	Invalid alias
178	Cannot unregister others
179	Quality of service control is not supported
180	Incomplete address
181	Registration permissions have expired
182	Call routed to SCN
183	Inconsistent alias
203	Call rejected at destination
208	Incorrect address
221	The far end is busy
222	The far end is not responding

System Security and Port Usage

This section provides an overview of the port usage and security required by the Polycom® Converged Management Application™ (CMA®) system and includes a comprehensive list of services and clients on the system that are required for normal operation. It includes these topics:

- [Open Inbound Ports on the Polycom CMA System](#)
- [Outbound Ports Used by the Polycom CMA System](#)

Open Inbound Ports on the Polycom CMA System

The following table lists the open inbound ports on the CMA system and provides a description of their use.

Port	Description
TCP 80	HTTP web server, through which the web application displays and where Polycom endpoints post status messages
TCP/UDP 161	SNMP listener
TCP 389	Directory services (LDAP)
TCP 443	HTTPS web server listener
TCP 700	(Polycom proprietary service) Service monitor for redundant Polycom CMA servers
TCP/UDP 1718	H.323 gatekeeper listener--gatekeeper discovery
TCP/UDP 1719	H.323 gatekeeper listener--gatekeeper statistics
TCP/UDP 1720	H.323 gatekeeper listener--host call
TCP 3601	(Polycom proprietary service) Global Address Book listener with which endpoints register
TCP 3389	Remote desktop
TCP 5222	Presence service (XMPP)

Port	Description
TCP 4449	(Polycom proprietary service) OpenDS (Data store for site topology) admin port
TCP 8989	(Polycom proprietary service) OpenDS (Data store for site topology) replication port

Note

Third-party port-scanning software may incorrectly identify the Polycom proprietary services as IANA-registered services, since identification is made by port number only and not by the actual protocol being transmitted:

Outbound Ports Used by the Polycom CMA System

The following table lists all outbound ports that the CMA system uses to communicate with other systems, including endpoints, bridges, database servers, and other network equipment.

As a standard H.323 gatekeeper, the CMA system uses ports 1024-65535 for dynamic TCP and UDP traffic.

Port	Description
TCP 20	Used to FTP data to endpoints.
TCP 21	
TCP/UDP 24	Used to access the telnet interfaces on endpoints.
TCP/UDP 25	Used to send E-mail messages to SMTP servers.
TCP/UDP 53	Used to access domain name servers (DNS).
TCP 80	Used to access the web application on endpoints and MGCs, version 7.x and higher.
TCP 135 TCP 137 TCP 139	Active Directory (AD) Single Signon (NetBios/NTLM).
TCP/UDP 389	Used to access directory (LDAP) services
TCP 443	Secure access to endpoint devices (SSL) including Polycom CMA Desktop.
TCP 445	AD Single Signon
TCP/UDP 636	Used to access LDAP over TLS/SSL (LDAPS)
TCP 1205	Used to access MGCs for management and monitoring

Port	Description
TCP/UDP 1719	Used by the gatekeeper for H.323 RAS messages
TCP/UDP 1720	Used by the gatekeeper for Q.931 signaling
TCP/UDP 3268	Used to access the Microsoft Active Directory Global Catalog using StartTLS.
TCP/UDP 3269	Used to access the Microsoft Active Directory Global Catalog using LDAP-S.
TCP/UDP 3603	Used for HTTP communication with the Polycom PVX client
TCP 5001 TCP 1205	Used to access MGCs for management and monitoring

